JOINT APPENDIX
VOLUME I

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

OFFICE OF FOREIGN ASSETS CONTROL

Case ID CYBER2-28475

DESIGNATION AND BLOCKING MEMORANDUM

The Office of Foreign Assets Control, pursuant to Executive Order 13694 of April 1, 2015, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," as amended by Executive Order 13757 of December 28, 2016, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities" (E.O. 13694, as amended), Executive Order 13722 of March 15, 2016, "Blocking Property of the Government of North Korea and the Workers' Party of Korea, and Prohibiting Certain Transactions with Respect to North Korea" (E.O. 13722), section 203 of the International Emergency Economic Powers Act (50 U.S.C. § 1702) (IEEPA), the National Emergencies Act (50 U.S.C. § 1601 et seq.), section 301 of title 3, United States Code, section 578.802 of the Cyber-Related Sanctions Regulations, 31 C.F.R. part 578, and section 510.802 of the North Korea Sanctions Regulations, 31 C.F.R. part 510, determines, after consultation with the Attorney General and the Secretary of State, that there is reason to believe the entity identified below and in the attached evidentiary memorandum meets one or more criteria for designation set forth in E.O. 13694, as amended, and E.O. 13722, and, therefore, is designated as a Specially Designated National or Blocked Person.

Entity

TORNADO CASH is an entity—that is, a "partnership, association, trust, joint venture, corporation, group, subgroup, or other organization"—that may be designated pursuant to IEEPA. **TORNADO CASH** is an entity with an organizational structure that consists of: (1) its founders – Alexey Pertsev, Roman Semenov, and Roman Storm – and other associated developers, who together launched the Tornado Cash mixing service, developed new Tornado Cash mixing service features, created the Tornado Cash Decentralized Autonomous Organization (DAO), and actively promote the platform's popularity in an attempt to increase its user base; and (2) the Tornado Cash DAO, which is responsible for voting on and implementing those new features created by the developers. **TORNADO CASH** is identified with the following identifiers listed below:

1. TORNADO CASH; Website tornado.cash; Digital Currency Address - ETH 0x12D66f87A04A9E220743712cE6d9bB1B5616B8Fc; alt. Digital Currency Address - ETH 0x47CE0C6eD5B0Ce3d3A51fdb1C52DC66a7c3c2936; alt. Digital Currency Address - ETH 0x910Cbd523D972eb0a6f4cAe4618aD62622b39DbF; alt. Digital Currency Address - ETH 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291; alt. Digital Currency Address - ETH 0xD4B88Df4D29F5CedD6857912842cff3b20C8Cfa3; alt. Digital Currency Address - ETH 0xFD8610d20aA15b7B2E3Be39B396a1bC3516c7144; alt. Digital

Currency Address - ETH 0x07687e702b410Fa43f4cB4Af7FA097918ffD2730; alt. Digital Currency Address - ETH 0x23773E65ed146A459791799d01336DB287f25334; alt. Digital Currency Address - ETH 0x22aaA7720ddd5388A3c0A3333430953C68f1849b; alt. Digital Currency Address - ETH 0x03893a7c7463AE47D46bc7f091665f1893656003; alt. Digital Currency Address - ETH 0x2717c5e28cf931547B621a5dddb772Ab6A35B701; alt. Digital Currency Address - ETH 0xD21be7248e0197Ee08E0c20D4a96DEBdaC3D20Af; alt. Digital Currency Address - ETH 0x4736dCf1b7A3d580672CcE6E7c65cd5cc9cFBa9D; alt. Digital Currency Address - ETH 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384; alt. Digital Currency Address - ETH 0xd96f2B1c14Db8458374d9Aca76E26c3D18364307; alt. Digital Currency Address - ETH 0x169AD27A470D064DEDE56a2D3ff727986b15D52B; alt. Digital Currency Address - ETH 0x0836222F2B2B24A3F36f98668Ed8F0B38D1a872f; alt. Digital Currency Address - ETH 0x178169B423a011fff22B9e3F3abeA13414dDD0F1; alt. Digital Currency Address - ETH 0x610B717796ad172B316836AC95a2ffad065CeaB4; alt. Digital Currency Address - ETH 0xbB93e510BbCD0B7beb5A853875f9eC60275CF498; alt. Digital Currency Address - ETH 0x84443CFd09A48AF6eF360C6976C5392aC5023a1F; alt. Digital Currency Address - ETH 0xd47438C816c9E7f2E2888E060936a499Af9582b3; alt. Digital Currency Address - ETH 0x330bdFADE01eE9bF63C209Ee33102DD334618e0a; alt. Digital Currency Address - ETH 0x1E34A77868E19A6647b1f2F47B51ed72dEDE95DD; alt. Digital Currency Address - ETH 0xdf231d99Ff8b6c6CBF4E9B9a945CBAcEF9339178; alt. Digital Currency Address - ETH 0xaf4c0B70B2Ea9FB7487C7CbB37aDa259579fe040; alt. Digital Currency Address - ETH 0xa5C2254e4253490C54cef0a4347fddb8f75A4998; alt. Digital Currency Address - ETH 0xaf8d1839c3c67cf571aa74B5c12398d4901147B3; alt. Digital Currency Address - ETH 0x6Bf694a291DF3FeC1f7e69701E3ab6c592435Ae7; alt. Digital Currency Address - ETH 0x3aac1cC67c2ec5Db4eA850957b967Ba153aD6279; alt. Digital Currency Address - ETH 0x723B78e67497E85279CB204544566F4dC5d2acA0; alt. Digital Currency Address - ETH 0x0E3A09dDA6B20aFbB34aC7cD4A6881493f3E7bf7; alt. Digital Currency Address - ETH 0x76D85B4C0Fc497EeCc38902397aC608000A06607; alt. Digital Currency Address - ETH 0xCC84179FFD19A1627E79F8648d09e095252Bc418; alt. Digital Currency Address - ETH 0xD5d6f8D9e784d0e26222ad3834500801a68D027D; alt. Digital Currency Address - ETH 0x407CcEeaA7c95d2FE2250Bf9F2c105aA7AAFB512; alt. Digital Currency Address - ETH 0x833481186f16Cece3f1Eeea1a694c42034c3a0dB; alt. Digital Currency Address - ETH 0xd8D7DE3349ccaA0Fde6298fe6D7b7d0d34586193; alt. Digital Currency Address - ETH 0x8281Aa6795aDE17C8973e1aedcA380258Bc124F9; alt. Digital Currency Address - ETH 0x57b2B8c82F065de8Ef5573f9730fC1449B403C9f; alt. Digital Currency Address - ETH 0x05E0b5B40B7b66098C2161A5EE11C5740A3A7C45; alt. Digital Currency Address - ETH 0x23173fE8b96A4Ad8d2E17fB83EA5dcccdCa1Ae52; alt. Digital Currency Address - ETH 0x538Ab61E8A9fc1b2f93b3dd9011d662d89bE6FE6; alt. Digital Currency Address - ETH

0x94Be88213a387E992Dd87DE56950a9aef34b9448; alt. Digital Currency Address - ETH 0x242654336ca2205714071898f67E254EB49ACdCe; alt. Digital Currency Address - ETH 0x776198CCF446DFa168347089d7338879273172cF; alt. Digital Currency Address - ETH 0xeDC5d01286f99A066559F60a585406f3878a033e; alt. Digital Currency Address - ETH 0xD692Fd2D0b2Fbd2e52CFa5B5b9424bC981C30696; alt. Digital Currency Address - ETH 0xca0840578f57fe71599d29375e16783424023357; alt. Digital Currency Address - ETH 0xDF3A408c53E5078af6e8fb2A85088D46Ee09A61b; alt. Digital Currency Address - ETH 0x743494b60097A2230018079c02fe21a7B687EAA5; alt. Digital Currency Address - ETH 0x94C92F096437ab9958fC0A37F09348f30389Ae79; alt. Digital Currency Address - ETH 0x5efda50f22d34F262c29268506C5Fa42cB56A1Ce; alt. Digital Currency Address - ETH 0x2f50508a8a3d323b91336fa3ea6ae50e55f32185; alt. Digital Currency Address - ETH 0xCEe71753C9820f063b38FDbE4cFDAf1d3D928A80; alt. Digital Currency Address - ETH 0xffbac21a641dcfe4552920138d90f3638b3c9fba; alt. Digital Currency Address - ETH 0x179f48c78f57a3a78f0608cc9197b8972921d1d2; alt. Digital Currency Address - ETH 0xb04E030140b30C27bcdfaafFFA98C57d80eDa7B4; alt. Digital Currency Address - ETH 0x77777feddddffc19ff86db637967013e6c6a116c; alt. Digital Currency Address - ETH 0x3efa30704d2b8bbac821307230376556cf8cc39e; alt. Digital Currency Address - ETH 0x746aebc06d2ae31b71ac51429a19d54e797878e9; alt. Digital Currency Address - ETH 0xd90e2f925DA726b50C4Ed8D0Fb90Ad053324F31b; alt. Digital Currency Address - ETH 0x5f6c97C6AD7bdd0AE7E0Dd4ca33A4ED3fDabD4D7; alt. Digital Currency Address - ETH 0xf4B067dD14e95Bab89Be928c07Cb22E3c94E0DAA; alt. Digital Currency Address - ETH 0x58E8dCC13BE9780fC42E8723D8EaD4CF46943dF2; alt. Digital Currency Address - ETH 0x01e2919679362dFBC9ee1644Ba9C6da6D6245BB1; alt. Digital Currency Address - ETH 0x2FC93484614a34f26F7970CBB94615bA109BB4bf; alt. Digital Currency Address - ETH 0x26903a5a198D571422b2b4EA08b56a37cbD68c89; alt. Digital Currency Address - ETH 0xB20c66C4DE72433F3cE747b58B86830c459CA911; alt. Digital Currency Address - ETH 0x2573BAc39EBe2901B4389CD468F2872cF7767FAF; alt. Digital Currency Address - ETH 0x527653eA119F3E6a1F5BD18fbF4714081D7B31ce; alt. Digital Currency Address - ETH 0x653477c392c16b0765603074f157314Cc4f40c32; alt. Digital Currency Address - ETH 0x88fd245fEdeC4A936e700f9173454D1931B4C307; alt. Digital Currency Address - ETH 0x09193888b3f38C82dEdfda55259A82C0E7De875E; alt. Digital Currency Address - ETH 0x5cab7692D4E94096462119ab7bF57319726Eed2A; alt. Digital Currency Address - ETH 0x756C4628E57F7e7f8a459EC2752968360Cf4D1AA; alt. Digital Currency Address - ETH 0x722122dF12D4e14e13Ac3b6895a86e84145b6967; alt. Digital Currency Address - ETH 0x94A1B5CdB22c43faab4AbEb5c74999895464Ddaf; alt. Digital Currency Address - ETH 0xb541fc07bC7619fD4062A54d96268525cBC6FfEF; alt. Digital Currency Address - ETH 0xD82ed8786D7c69DC7e052F7A542AB047971E73d2; alt. Digital Currency Address - ETH 0xF67721A2D8F736E75a49FdD7FAd2e31D8676542a; alt. Digital Currency

Address - ETH 0x9AD122c22B14202B4490eDAf288FDb3C7cb3ff5E; alt. Digital Currency Address - ETH 0xD691F27f38B395864Ea86CfC7253969B409c362d; alt. Digital Currency Address - ETH 0xaEaaC358560e11f52454D997AAFF2c5731B6f8a6; alt. Digital Currency Address - ETH 0x1356c899D8C9467C7f71C195612F8A395aBf2f0a; alt. Digital Currency Address - ETH 0xA60C772958a3eD56c1F15dD055bA37AC8e523a0D; alt. Digital Currency Address - ETH 0xBA214C1c1928a32Bffe790263E38B4Af9bFCD659; alt. Digital Currency Address - ETH 0xb1C8094B234DcE6e03f10a5b673c1d8C69739A00; alt. Digital Currency Address - ETH 0xF60dD140cFf0706bAE9Cd734Ac3ae76AD9eBC32A; alt. Digital Currency Address - ETH 0x8589427373D6D84E98730D7795D8f6f8731FDA16; Secondary sanctions risk: North Korea Sanctions Regulations, sections 510.201 and 510.210; Transactions Prohibited For Persons Owned or Controlled By U.S. Financial Institutions: North Korea Sanctions Regulations section 510.214; Organization Established Date 2019 [DPRK3] [CYBER2].

Accordingly, except to the extent otherwise provided by law or unless licensed or otherwise authorized by the Office of Foreign Assets Control, (1) all real, personal, and any other property and interests in property of the entity named above that are or hereafter come within the United States, or that are or hereafter come within the possession or control of any U.S. person are blocked and may not be transferred, paid, exported, withdrawn or otherwise dealt in, and (2) any transaction or dealing by a U.S. person or within the United States in property or interests in property of the entity named above is prohibited.

Additionally, except to the extent otherwise provided by law or unless licensed or otherwise authorized by the Office of Foreign Assets Control, the following are prohibited: (1) any transaction by a United States person or within the United States that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate, any of the prohibitions set forth in the Order; and (2) any conspiracy formed to violate any of the prohibitions set forth in E.O. 13694, as amended, and E.O. 13722.

The President has found in Section 7 of E.O. 13694, as amended, that, because of the ability to transfer funds or other assets instantaneously, prior notice to persons designated pursuant to E.O. 13694, as amended, of measures to be taken pursuant to E.O. 13694, as amended, would render these measures ineffectual. Therefore, the President determined that there need be no prior notice of such a listing or determination. In making this determination pursuant to E.O. 13694, as amended, I also find that no prior notice should be afforded to the entity named above notwithstanding the entity's prior designation because to do so would provide an opportunity to evade the measures authorized by E.O. 13694, as amended, and, consequently, render those measures ineffectual towards addressing the national emergency declared in E.O. 13694, as amended.

The President has found in Section 10 of E.O. 13722 that, because of the ability to transfer funds or other assets instantaneously, prior notice to persons designated pursuant to E.O. 13722 of measures to be taken pursuant to E.O. 13722 would render these measures ineffectual. Therefore, the President determined that there need be no prior notice of such a listing or determination. In making this determination pursuant to E.O. 13722, I also find

that no prior notice should be afforded to the entity named above notwithstanding the entity's prior designation because to do so would provide an opportunity to evade the measures authorized by E.O. 13722 and, consequently, render those measures ineffectual towards addressing the national emergency declared in E.O. 13722.

November 8, 2022

Date

Andrea M. Gacki Digitally signed by Andrea M. Gacki Date: 2022.11.08 14:30:32 -05'00'

Andrea M. Gacki
Director
Office of Foreign Assets Control

date. However, DOT would reserve the right to modify or shorten the duration of this waiver if it obtains information before the end of the five-year period indicating the waiver is no longer in the public interest.

The Implementation Guidance also provides that, before granting a waiver in the public interest, to the extent permitted by law, agencies shall assess whether a significant portion of any cost advantage of a foreign-sourced product is "the result of the use of dumped steel, iron, or manufactured products or the use of injuriously subsidized steel, iron, or manufactured products." Implementation Guidance at p. 12. E.O. 14005 at Section 5 includes a similar requirement for "steel, iron, or manufactured goods." However, because the public interest waiver that DOT is proposing in this notice is not based on consideration of the cost advantage of any foreign-sourced steel, iron, or manufactured product content, there is not a specific cost advantage for DOT to consider.

DOT will consider all comments received in the initial 15-day comment period during our consideration of the proposed waiver, as required by section 70914(c)(2) of the BIL. Comments received after this period, but before notice of our finding is published in the **Federal Register**, will be considered to the extent practicable. Section 117 of the SAFETEA–LU Technical Corrections Act of 2008 (Pub. L. 110–244, 122 Stat. 1572) also requires an additional 5-day, comment period after FHWA publishes a waiver finding notice. Comments received during that period will be reviewed, but the finding will continue to remain valid. Those comments may influence DOT/FHWA's decision to terminate or modify a finding.

Issued in Washington, DC on: November 4, 2022.

Polly E. Trottenberg,

Deputy Secretary.

[FR Doc. 2022–24744 Filed 11–14–22; 8:45 am]

BILLING CODE 4910–9X–P

DEPARTMENT OF THE TREASURY

Office of Foreign Assets Control

Notice of OFAC Sanctions Action

AGENCY: Office of Foreign Assets Control, Treasury.

ACTION: Notice.

SUMMARY: The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is publishing the name of one entity that has been placed on OFAC's Specially Designated Nationals and Blocked Persons List based on OFAC's determination that one or more applicable legal criteria were satisfied. All property and interests in property subject to U.S. jurisdiction of this entity are blocked, and U.S. persons are generally prohibited from engaging in transactions with it.

DATES: See **SUPPLEMENTARY INFORMATION** section for effective date(s).

FOR FURTHER INFORMATION CONTACT: OFAC: Andrea M. Gacki, Director, tel.: 202–622–2490; Associate Director for Global Targeting, tel.: 202–622–2420; Assistant Director for Licensing, tel.: 202–622–2480; Assistant Director for Regulatory Affairs, tel.: 202–622–4855; or the Assistant Director for Sanctions Compliance & Evaluation, tel.: 202–622–2490.

SUPPLEMENTARY INFORMATION:

Electronic Availability

The Specially Designated Nationals and Blocked Persons List and additional information concerning OFAC sanctions programs are available on OFAC's website (*https://www.treasury.gov/ofac*).

Notice of OFAC Action

On November 8, 2022, OFAC determined that the property and interests in property subject to U.S. jurisdiction of the following entity are blocked under the relevant sanctions authorities listed below.

Entity

1. TORNADO CASH; website *tornado.cash;* Digital Currency Address—ETH 0x12D66f87A04A9E220743712cE6d9bB1B5616B8Fc; alt. Digital Currency Address—ETH 0x47CE0C6eD5B0Ce3d3A51fdb1C52DC66a7c3c2936; alt. Digital Currency Address—ETH 0x910Cbd523D972eb0a6f4cAe4618aD62622b39DbF; alt. Digital Currency Address—ETH 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291; alt. Digital Currency Address—ETH 0xD4B88Df4D29F5CedD6857912842cff3b20C8Cfa3; alt. Digital Currency Address—ETH 0xFD8610d20aA15b7B2E3Be39B396a1bC3516c7144; alt. Digital Currency Address—ETH 0x07687e702b410Fa43f4cB4Af7FA097918ffD2730; alt. Digital Currency Address—ETH 0x23773E65ed146A459791799d01336DB287f25334; alt. Digital Currency Address—ETH 0x22aaA7720ddd5388A3c0A3333430953C68f1849b; alt. Digital Currency Address—ETH 0x03893a7c7463AE47D46bc7f091665f1893656003; alt. Digital Currency Address—ETH 0x2717c5e28cf931547B621a5dddb772Ab6A35B701; alt. Digital Currency Address—ETH 0xD21be7248e0197Ee08E0c20D4a96DEBdaC3D20Af; alt. Digital Currency Address—ETH 0x4736dCf1b7A3d580672CcE6E7c65cd5cc9cFBa9D; alt. Digital Currency Address—ETH 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384; alt. Digital Currency Address—ETH 0xd96f2B1c14Db8458374d9Aca76E26c3D18364307; alt. Digital Currency Address—ETH 0x169AD27A470D064DEDE56a2D3ff727986b15D52B; alt. Digital Currency Address—ETH 0x0836222F2B2B24A3F36f98668Ed8F0B38D1a872f; alt. Digital Currency Address—ETH 0x178169B423a011fff22B9e3F3abeA13414dDD0F1; alt. Digital Currency Address—ETH 0x610B717796ad172B316836AC95a2ffad065CeaB4; alt. Digital Currency Address—ETH 0xbB93e510BbCD0B7beb5A853875f9eC60275CF498; alt. Digital Currency Address—ETH 0x84443CFd09A48AF6eF360C6976C5392aC5023a1F; alt. Digital Currency Address—ETH 0xd47438C816c9E7f2E2888E060936a499Af9582b3; alt. Digital Currency Address—ETH 0x330bdFADE01eE9bF63C209Ee33102DD334618e0a; alt. Digital Currency Address—ETH 0x1E34A77868E19A6647b1f2F47B51ed72dEDE95DD; alt. Digital Currency Address—ETH 0xdf231d99Ff8b6c6CBF4E9B9a945CBAcEF9339178; alt. Digital Currency Address—ETH 0xaf4c0B70B2Ea9FB7487C7CbB37aDa259579fe040; alt. Digital Currency Address—ETH 0xa5C2254e4253490C54cef0a4347fddb8f75A4998; alt. Digital Currency Address—ETH 0xaf8d1839c3c67cf571aa74B5c12398d4901147B3; alt. Digital Currency Address—ETH 0x6Bf694a291DF3FeC1f7e69701E3ab6c592435Ae7; alt. Digital Currency Address—ETH 0x3aac1cC67c2ec5Db4eA850957b967Ba153aD6279; alt. Digital Currency Address—ETH 0x723B78e67497E85279CB204544566F4dC5d2acA0; alt. Digital Currency Address—ETH 0x0E3A09dDA6B20aFbB34aC7cD4A6881493f3E7bf7; alt. Digital Currency Address—ETH 0x76D85B4C0Fc497EeCc38902397aC608000A06607; alt. Digital Currency Address—ETH 0xCC84179FFD19A1627E79F8648d09e095252Bc418; alt. Digital Currency Address—ETH 0xD5d6f8D9e784d0e26222ad3834500801a68D027D; alt. Digital Currency Address—ETH

0x407CcEeaA7c95d2FE22 50Bf9F2c105aA7AAFB512; alt. Digital Currency Address—ETH 0x833481186f16Cece 3f1Eeea1a694c42034c3a0dB; alt. Digital Currency Address—ETH 0xd8D7DE3349ccaA0F de6298fe6D7b7d0d34586193; alt. Digital Currency Address—ETH 0x8281Aa6795aDE17C8 973e1aedcA380258Bc124F9; alt. Digital Currency Address—ETH 0x57b2B8c82F065de8Ef 5573f9730fC1449B403C9f; alt. Digital Currency Address—ETH 0x05E0b5B40B7b66098 C2161A5EE11C5740A3A7C45; alt. Digital Currency Address—ETH 0x23173fE8b96A4Ad8d2 E17fB83EA5dcccdCa1Ae52; alt. Digital Currency Address—ETH 0x538Ab61E8A9fc1b2f93 b3dd9011d662d89bE6FE6; alt. Digital Currency Address—ETH 0x94Be88213a387E992 Dd87DE56950a9aef34b9448; alt. Digital Currency Address—ETH 0x242654336ca22057 14071898f67E254EB49ACdCe; alt. Digital Currency Address—ETH 0x776198CCF446DFa168 347089d7338879273172cF; alt. Digital Currency Address—ETH 0xeDC5d01286f99A0665 59F60a585406f3878a033e; alt. Digital Currency Address—ETH 0xD692Fd2D0b2Fbd2e52 CFa5B5b9424bC981C30696; alt. Digital Currency Address—ETH 0xca0840578f57fe71599 d29375e16783424023357; alt. Digital Currency Address—ETH 0xDF3A408c53E5078af6e8 fb2A85088D46Ee09A61b; alt. Digital Currency Address—ETH 0x743494b60097A223001 8079c02fe21a7B687EAA5; alt. Digital Currency Address—ETH 0x94C92F096437ab9958f C0A37F09348f30389Ae79; alt. Digital Currency Address—ETH 0x5efda50f22d34F262c 29268506C5Fa42cB56A1Ce; alt. Digital Currency Address—ETH 0x2f50508a8a3d323b 91336fa3ea6ae50e55f32185; alt. Digital Currency Address—ETH 0xCEe71753C9820f063b 38FDbE4cFDAf1d3D928A80; alt. Digital Currency Address—ETH 0xffbac21a641dcfe455 2920138d90f3638b3c9fba; alt. Digital Currency Address—ETH 0x179f48c78f57a3a78f 0608cc9197b8972921d1d2; alt. Digital Currency Address—ETH 0xb04E030140b30C27bcdf aafFFA98C57d80eDa7B4; alt. Digital Currency Address—ETH 0x77777feddddffc19ff86 db637967013e6c6a116c; alt. Digital Currency Address—ETH 0x3efa30704d2b8bbac82 1307230376556cf8cc39e; alt. Digital Currency Address—ETH 0x746aebc06d2ae31b71ac 51429a19d54e797878e9; alt. Digital Currency Address—ETH 0xd90e2f925DA726b50C4E d8D0Fb90Ad053324F31b; alt. Digital Currency Address—ETH 0x5f6c97C6AD7bdd0AE7E0 Dd4ca33A4ED3fDabD4D7; alt. Digital Currency Address—ETH 0xf4B067dD14e95Bab89Be 928c07Cb22E3c94E0DAA; alt. Digital Currency Address—ETH 0x58E8dCC13BE9780fC42E 8723D8EaD4CF46943dF2; alt. Digital Currency Address—ETH 0x01e2919679362dFBC9ee 1644Ba9C6da6D6245BB1; alt. Digital Currency Address—ETH 0x2FC93484614a34f26F 7970CBB94615bA109BB4bf; alt. Digital Currency Address—ETH 0x26903a5a198D571422b 2b4EA08b56a37cbD68c89; alt. Digital Currency Address—ETH 0xB20c66C4DE72433F3c E747b58B86830c459CA911; alt. Digital Currency Address—ETH 0x2573BAc39EBe2901B 4389CD468F2872cF7767FAF; alt. Digital Currency Address—ETH 0x527653eA119F3E6a1F5 BD18fbF4714081D7B31ce; alt. Digital Currency Address—ETH 0x653477c392c16b076560 3074f157314Cc4f40c32; alt. Digital Currency Address—ETH 0x88fd245fEdeC4A936e70 0f9173454D1931B4C307; alt. Digital Currency Address—ETH 0x09193888b3f38C82d Edfda55259A82C0E7De875E; alt. Digital Currency Address—ETH 0x5cab7692D4E940964 62119ab7bF57319726Eed2A; alt. Digital Currency Address—ETH 0x756C4628E57F7e7f8a 459EC2752968360Cf4D1AA; alt. Digital Currency Address—ETH 0x722122dF12D4e14e13Ac 3b6895a86e84145b6967; alt. Digital Currency Address—ETH 0x94A1B5CdB22c43faab 4AbEb5c74999895464Ddaf; alt. Digital Currency Address—ETH 0xb541fc07bC7619fD 4062A54d96268525cBC6FfEF; alt. Digital Currency Address—ETH 0xD82ed8786D7c69DC7e 052F7A542AB047971E73d2; alt. Digital Currency Address—ETH 0xDD4c48C0B24039969fC 16D1cdF626eaB821d3384; alt. Digital Currency Address—ETH 0xF67721A2D8F736E75a 49FdD7FAd2e31D8676542a; alt. Digital Currency Address—ETH 0x9AD122c22B14202B4490e DAf288FDb3C7cb3ff5E; alt. Digital Currency Address—ETH 0xD691F27f38B395864Ea86 CfC7253969B409c362d; alt. Digital Currency Address—ETH 0xaEaaC358560e11f52454 D997AAFF2c5731B6f8a6; alt. Digital Currency Address—ETH 0x1356c899D8C9467C7f71 C195612F8A395aBf2f0a; alt. Digital Currency Address—ETH 0xA60C772958a3eD56c1F 15dD055bA37AC8e523a0D; alt. Digital Currency Address—ETH 0xBA214C1c1928a32Bffe 790263E38B4Af9bFCD659; alt. Digital Currency Address—ETH 0xb1C8094B234DcE6e03f 10a5b673c1d8C69739A00; alt. Digital Currency Address—ETH 0xF60dD140cFf0706bAE9 Cd734Ac3ae76AD9eBC32A; alt. Digital Currency Address—ETH 0x8589427373D6D84E98 730D7795D8f6f8731FDA16; Secondary sanctions risk: North Korea Sanctions Regulations, sections 510.201 and 510.210; Transactions Prohibited For Persons Owned or Controlled By U.S. Financial Institutions: North Korea Sanctions Regulations section 510.214; Organization Established Date 2019 [DPRK3] [CYBER2].

Designated pursuant to section 1(a)(iii)(B) of Executive Order 13694 of April 1, 2015, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," 80 FR 18077, 3 CFR, 2015 Comp., p. 297, as amended by Executive Order 13757 of December 28, 2016, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," 82 FR 1, 3 CFR, 2016 Comp., p. 659 (E.O. 13694, as amended) for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, an activity described in section 1(a)(ii) of E.O. 13694, as amended.

Also designated pursuant to section 2(a)(vii) of Executive Order 13722 of March 15, 2016, "Blocking Property of the Government of North Korea and the Workers' Party of Korea, and Prohibiting Certain Transactions with Respect to North Korea," 81 FR 14943, 3 CFR, 2016 Comp., p. 446 (E.O. 13722), for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or

services to or in support of, any person whose property and interests in property are blocked pursuant to E.O. 13722.

Dated: November 8, 2022.

Andrea M. Gacki,

Director, Office of Foreign Assets Control, U.S. Department of the Treasury.

[FR Doc. 2022–24798 Filed 11–14–22; 8:45 am]

BILLING CODE 4810–AL–P

DEPARTMENT OF THE TREASURY

Office of Foreign Assets Control

Notice of OFAC Sanctions Actions

AGENCY: Office of Foreign Assets Control, Treasury.

ACTION: Notice.

SUMMARY: The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is publishing the names of one or more persons that have been placed on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) based on OFAC's determination that one or more applicable legal criteria were satisfied. All property and interests in property subject to U.S. jurisdiction of these persons are blocked, and U.S. persons are generally prohibited from engaging in transactions with them.

DATES: See **SUPPLEMENTARY INFORMATION** section for applicable date(s).

FOR FURTHER INFORMATION CONTACT: OFAC: Andrea Gacki, Director, tel.: 202–622–2490; Associate Director for Global Targeting, tel.: 202–622–2420; Assistant Director for Licensing, tel.: 202–622–2480; Assistant Director for Regulatory Affairs, tel.: 202–622–4855; or Assistant Director for Sanctions Compliance & Evaluation, tel.: 202–622–2490.

SUPPLEMENTARY INFORMATION:

Electronic Availability

The SDN List and additional information concerning OFAC sanctions programs are available on OFAC's website (*https://www.treasury.gov/ofac*).

Notice of OFAC Actions

On November 8, 2022, OFAC determined that the property and interests in property subject to U.S. jurisdiction of the following persons are blocked under the relevant sanctions authority listed below.

Individuals

1. OO, Kyaw Min, Yangon, Burma; DOB 18 Jan 1982; nationality Burma; Gender Male; National ID No. 14/MAMAKA N 140703 (Burma) (individual) [BURMA–EO14014].

Designated pursuant to section 1(a)(i) of Executive Order 14014 of February 10, 2021, "Blocking Property With Respect to the Situation in Burma" ("E.O. 14014"), 86 FR 9429, for operating in the defense sector of the Burmese economy or any other sector of the Burmese economy as may be determined by the Secretary of the Treasury, in consultation with the Secretary of State.

Entities

1. SKY AVIATOR COMPANY LIMITED (a.k.a. SKY AVIATOR CO.; a.k.a. SKY AVIATOR CO., LTD.; a.k.a. SKY AVIATOR COMPANY LTD.; a.k.a. "SKY AVIATOR"), No. 286, Bogyoke Street, Ward No. 2, Waibargi, North Okkalarpa Township, Yangon Region, Burma; No. 204/2, Myinthar 11th Street, Ward 14/1, South Okkalarpa Township, Yangon, Burma; Target Type Private Company; Business Registration Number 100789450 (Burma) [BURMA–EO14014].

Designated pursuant to section 1(a)(i) of E.O. 14014 for operating in the defense sector of the Burmese economy or any other sector of the Burmese economy as may be determined by the Secretary of the Treasury, in consultation with the Secretary of State.

Authority: E.O. 14014, 86 FR 9429.

Dated: November 8, 2022.

Andrea M. Gacki,

Director, Office of Foreign Assets Control, U.S. Department of the Treasury.

[FR Doc. 2022–24736 Filed 11–14–22; 8:45 am]

BILLING CODE 4810–AL–P

DEPARTMENT OF THE TREASURY

Office of Foreign Assets Control

Notice of OFAC Sanctions Actions

AGENCY: Office of Foreign Assets Control, Treasury.

ACTION: Notice.

SUMMARY: The Department of the Treasury's Office of Foreign Assets Control (OFAC) is publishing the names of one or more persons that have been placed on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) based on OFAC's determination that one or more applicable legal criteria were satisfied. All property and interests in property subject to U.S. jurisdiction of these persons are blocked, and U.S. persons are generally prohibited from engaging in transactions with them.

DATES: See **SUPPLEMENTARY INFORMATION** section for applicable date(s).

FOR FURTHER INFORMATION CONTACT: OFAC: Andrea Gacki, Director, tel.: 202–622–2490; Associate Director for Global Targeting, tel.: 202–622–2420; Assistant Director for Licensing, tel.: 202–622–2480; Assistant Director for Regulatory Affairs, tel.: 202–622–4855; or Assistant Director for Sanctions Compliance & Evaluation, tel.: 202–622–2490.

SUPPLEMENTARY INFORMATION:

Electronic Availability

The SDN List and additional information concerning OFAC sanctions programs are available on OFAC's website (*www.treasury.gov/ofac*).

Notice of OFAC Actions

On November 7, 2022, OFAC determined that the property and interests in property subject to U.S. jurisdiction of the following persons are blocked under the relevant sanctions authority listed below.

Individuals

1. RI, Sok, Dandong, China; DOB 28 Jul 1973; nationality Korea, North; Gender Male; Secondary sanctions risk: North Korea Sanctions Regulations, sections 510.201 and 510.210; Transactions Prohibited For Persons Owned or Controlled By U.S. Financial Institutions: North Korea Sanctions Regulations section 510.214 (individual) [DPRK3] (Linked To: AIR KORYO).

Designated pursuant to section 2(a)(viii) of Executive Order 13722 of March 15, 2016, "Blocking Property of the Government of North Korea and the Workers' Party of Korea, and Prohibiting Certain Transactions With Respect to North Korea," 81 FR 14943, 3 CFR, 2016 Comp., p. 446 (E.O. 13722 or the "Order"), for being owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, AIR KORYO, a person whose property and interests in property are blocked pursuant to the Order.

2. YAN, Zhiyong, Beijing, China; DOB 15 Feb 1980; POB Shandong, China; nationality China; Gender Male; Secondary sanctions risk: North Korea Sanctions Regulations, sections 510.201 and 510.210; Transactions Prohibited For Persons Owned or Controlled By U.S. Financial Institutions: North Korea Sanctions Regulations section 510.214; National ID No. 370827198002151333 (China) (individual) [DPRK3] (Linked To: AIR KORYO).

Designated pursuant to section 2(a)(viii) of E.O. 13722 for being owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, AIR KORYO, a person whose property and interests in property are blocked pursuant to the Order.

Authority: E.O. 13722, 81 FR 14943, 3 CFR, 2016 Comp., p. 446.

Dated: November 7, 2022.

Andrea Gacki,

Director, Office of Foreign Assets Control, U.S. Department of the Treasury.

[FR Doc. 2022–24737 Filed 11–14–22; 8:45 am]

BILLING CODE 4810–AL–P

U.S. DEPARTMENT OF THE TREASURY

Treasury Designates DPRK Weapons Representatives

November 8, 2022

Tornado Cash Redesignated with Additional DPRK Authorities, New OFAC Guidance

WASHINGTON – Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is designating two individuals for engaging in transportation and procurement activities on behalf of the Democratic People's Republic of Korea (DPRK). These individuals have acted on behalf of Air Koryo, an entity previously designated by OFAC for operating in the transportation industry in the DPRK economy. OFAC also delisted and simultaneously redesignated Tornado Cash under Executive Order (E.O.) 13722 and E.O. 13694, as amended. The redesignation takes into account additional information and also includes an additional basis for the designation of Tornado Cash regarding its support for DPRK activities. Tornado Cash, an entity that provides virtual currency mixing services, obfuscated the movement of over $455 million stolen in March 2022 by the OFAC-designated, DPRK-controlled Lazarus Group in the largest known virtual currency heist to date. OFAC also issued a new Frequently Asked Question (FAQ) to provide additional compliance guidance regarding the nature of the Tornado Cash entity, and updated three existing FAQs with additional guidance.

This action is part of the United States' ongoing efforts to limit the DPRK's ability to advance its unlawful weapons of mass destruction (WMD) and ballistic missile programs that threaten regional stability and follows numerous recent DPRK ballistic missile launches, which are in clear violation of multiple United Nations (UN) Security Council resolutions. Continued provocation by the DPRK exemplifies the threat its unlawful weapons and missile programs pose to its neighbors, the region, international peace and security, and the global non-proliferation regime.

"Today's sanctions action targets two key nodes of the DPRK's weapons programs: its increasing reliance on illicit activities, including cybercrime, to generate revenue, and its ability to procure and transport goods in support of weapons of mass destruction and ballistic missile programs," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson.

INDIVIDUALS FACILITATING THE DPRK'S BALLISTIC MISSILE AND WEAPONS PROGRAMS

Air Koryo is the DPRK's national flag carrier and reportedly continues to own and operate all civilian aircraft registered in the DPRK. Air Koryo previously transported parts used in Scud-B missile systems, which fall under a UN prohibition on exporting arms and related materiel to the DPRK. According to a UN report, Air Koryo is controlled by and integrated into the DPRK military and the airline's assets are actively utilized for military purposes.

Ri Sok, an Air Koryo representative in Dandong, China, was involved in the transportation of electronic parts from China to the DPRK on behalf of the DPRK's Ministry of Rocket Industry (MORI). OFAC designated MORI on April 1, 2022 for being owned or controlled by the Munitions Industry Department (MID), an entity designated on August 30, 2010 pursuant to E.O. 13382 for its involvement with or provision of support for the DPRK's WMD and ballistic missile programs. The MID, which oversees the DPRK's ballistic missile development and nuclear weapons program, was designated by the UN on March 2, 2016.

Yan Zhiyong is a logistics manager with Air Koryo and facilitates the transportation of goods to the DPRK. Specifically, Yan Zhiyong transported goods from China to the DPRK on behalf of the Reconnaissance General Bureau (RGB), the DPRK's principal intelligence agency. The RGB, which is also involved in the DPRK's arms trade, was designated on January 2, 2015 pursuant to E.O. 13687 for being a controlled entity of the Government of the DPRK. The RGB was designated by the UN on March 2, 2016. Yan Zhiyong was the primary point of contact and intermediary for shipments destined for the DPRK and has used a Beijing-based company to transport goods into the DPRK.

Ri Sok and Yan Zhiyong are designated pursuant to E.O. 13722 for acting or purporting to act for or on behalf of, directly or indirectly, Air Koryo, a person whose property and interests in property are blocked pursuant to E.O. 13722 and who has ties to the DPRK's military activities.

REDESIGNATING TORNADO CASH

In addition to the Air Koryo representatives, OFAC simultaneously delisted and redesignated **Tornado Cash** under E.O. 13722 and E.O. 13694, as amended, for its role in enabling malicious cyber activities, which ultimately support the DPRK's WMD program. Effective immediately, the August 8, 2022 designation of Tornado Cash is no longer operative, and it is wholly replaced by today's action.

Tornado Cash is an entity that provides virtual currency mixing services through smart contracts that primarily operate on the Ethereum blockchain. The Tornado Cash smart contracts are a form of computer code that Tornado Cash uses to implement its governance structure, provide mixing services, offer financial incentives for users, increase its user base, and facilitate the financial gain of its users and developers. These smart contracts have been used by actors to obfuscate the source of funds derived from cyber heists, including funds stolen by Lazarus Group in March 2022. Malicious cyber actors subsequently used the Tornado Cash smart contracts to launder more than $96 million of funds derived from the June 24, 2022 Harmony Bridge Heist, and at least $7.8 million from the August 2, 2022 Nomad Heist.

Lazarus Group used the Tornado Cash smart contracts to obfuscate the source of funds derived from the March 2022 cyber heist. Lazarus Group was designated on September 13, 2019 pursuant to E.O. 13722 for being an agency, instrumentality, or controlled entity of the RGB, which has been identified as part of the Government of the DPRK. Today, OFAC is sanctioning Tornado Cash pursuant to E.O. 13722 for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, the Government of the DPRK, a person whose property and interests in property are blocked pursuant to E.O. 13722.

OFAC is also redesignating Tornado Cash pursuant to E.O. 13694, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain. Specifically, the smart contracts through which Tornado Cash operates were used to obfuscate the source and destination of funds derived from Lazarus Group's March 2022 cyber heist.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the individuals and entity designated today that are in the United States or in the possession or control of U.S. persons must be blocked and reported to OFAC. OFAC's regulations generally prohibit all dealings by

U.S. persons or within the United States (including transactions transiting the United States) that involve any property or interests in property of blocked or designated persons.

In addition, persons that engage in certain transactions with the individuals or entities designated today may themselves be exposed to designation. Furthermore, any foreign financial institution that knowingly facilitates a significant transaction or provides significant financial services for any of the individuals or entities designated today could be subject to U.S. correspondent or payable-through account sanctions.

The power and integrity of OFAC sanctions derive not only from its ability to designate and add persons to the Specially Designated Nationals and Blocked Persons (SDN) List but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer to OFAC's Frequently Asked Question 897. For detailed information on the process to submit a request for removal from an OFAC sanctions list, please refer to OFAC's website.

For additional information and guidance regarding sanctions implications specific to Tornado Cash, please reference OFAC's FAQs 1076–1079 and FAQ 1095.

For information on complying with virtual currency-related sanctions, please see OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry here and OFAC's FAQs on virtual currency here.

For more information on the individuals and entity designated today, click here.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

OFFICE OF FOREIGN ASSETS CONTROL

CYBER2–28475

EVIDENTIARY MEMORANDUM

MEMORANDUM FOR: Andrea M. Gacki
Director
Office of Foreign Assets Control

THROUGH: Ripley Quinby
Deputy Associate Director
Office of Global Targeting

[redacted]
Assistant Director
Russia, Europe, and Cyber Division

FROM: [redacted]
Acting Section Chief
Cyber and Virtual Assets Section

[redacted]
Sanctions Investigator
Cyber and Virtual Assets Section

[redacted]
Sanctions Investigator
Russia and Europe Section

SUBJECT: (U//~~FOUO~~) **TORNADO CASH**: Designation Pursuant to Executive Order 13694 of April 1, 2015, as amended by Executive Order 13757 of December 28, 2016; and Executive Order 13722 of March 15, 2016

I. (U) INTRODUCTION

(U) On April 1, 2015, the President issued Executive Order (E.O.) 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." [Exhibit 99]

(U) On December 28, 2016, the President issued E.O. 13757, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities." [Exhibit 45]

(U) E.O. 13694, as amended by E.O. 13757 ("E.O. 13694, as amended"), blocks the property and interests in property of any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to meet one or more of the criteria of the Order. [Exhibit 99] [Exhibit 45]

(U) On March 15, 2016, the President issued E.O. 13722, "Blocking Property of the Government of North Korea and the Workers' Party of Korea, and Prohibiting Certain Transactions with Respect to North Korea." [Exhibit 100]

(U) E.O. 13722 blocks the property and interests in property of the GOVERNMENT OF NORTH KOREA* (the "GONK*"),[1] the WORKERS' PARTY OF KOREA* (WPK*), and of any person determined by the Secretary of the Treasury, in consultation with the Secretary of State, to meet one or more of the designation criteria of E.O. 13722. [Exhibit 100]

(U) The Office of Foreign Assets Control (OFAC) previously designated **TORNADO CASH** on August 8, 2022, pursuant to E.O. 13694, as amended; [2] OFAC has rescinded that designation, and OFAC has redesignated **TORNADO CASH** on the basis of the information cited herein and in the accompanying classified addendum. The redesignation takes account of additional information and includes an additional basis for the designation of **TORNADO CASH**.

(U//~~FOUO~~) **Cyber-Enabled Activities**: Based on information presented in this memorandum and the accompanying exhibits, OFAC assesses that the ***Sky Mavis-Ronin Bridge Heist***[3] is a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain, and thus meets the criteria for designation pursuant to section 1(a)(ii)(D) of E.O. 13694, as amended.

(U) **Material Support for Cyber-Enabled Activities**: Based on information presented in this memorandum and the accompanying exhibits, OFAC assesses that **TORNADO CASH** has materially assisted, sponsored, or provided financial, material, or technological support for, or

---

[1] (U) E.O. 13722 defines the GONK* to include the Government of the Democratic People's Republic of Korea (DPRK) and its agencies, instrumentalities, and controlled entities. Section 510.311 of OFAC's North Korea Sanctions Regulations, 31 C.F.R. Part 510, defines the GONK* to include, *inter alia*, (a) the state and Government of the DPRK, as well as any political subdivision, agency, or instrumentality thereof, and (b) any entity owned or controlled, directly or indirectly, by any of the foregoing, including any corporation, partnership, association, or other entity in which the GONK* owns a 50 percent or greater interest or a controlling interest, and any entity which is otherwise controlled by the GONK*.

[2] (U) On August 8, 2022, the U.S. Department of the Treasury designated **TORNADO CASH** pursuant to E.O. 13694, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain. [Exhibit 202, p. 2]

[3] (U) Throughout this memorandum, the names of targets proposed for designation will appear in **BOLD CAPITAL** letters, the name of a cyber-enabled activity described in E.O. 13694, as amended, will appear in ***Bold Italics***, and an asterisk (*) following a name in ALL CAPS denotes an individual or entity whose property and interests in property have been blocked.

goods or services to or in support of, the ***Sky Mavis-Ronin Bridge Heist***, an activity described in section 1(a)(ii) of E.O. 13694, as amended, and thus meets the criteria for designation pursuant to section 1(a)(iii)(B) of E.O. 13694, as amended.

(U//~~FOUO~~) **DPRK:** Based on information presented in this memorandum and the accompanying exhibits, OFAC assesses that **TORNADO CASH** has materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of the GONK*, a person whose property and interests in property are blocked pursuant to E.O. 13722, and thus meets the criteria for designation pursuant to section 2(a)(vii) of E.O. 13722.

(U) For these reasons, **TORNADO CASH** should be added to the List of Specially Designated Nationals and Blocked Persons (the "SDN List") pursuant to E.O. 13694, as amended, and E.O. 13722.

II. (U) EXECUTIVE SUMMARY

(U) OFAC has designated **TORNADO CASH** for materially supporting the ***Sky Mavis-Ronin Bridge Heist*** and the GOVERNMENT OF NORTH KOREA* (GONK*). As part of the ***Sky Mavis-Ronin Bridge Heist***, cyber actors associated with GONK* stole over $600 million in ether (a virtual currency) from Sky Mavis, the Vietnam-based producer of a popular online game. OFAC assesses that cyber actors responsible for the ***Sky Mavis-Ronin Bridge Heist*** then used the Tornado Cash virtual asset mixing service, to launder the proceeds. GONK* uses funds derived from such malicious cyber activities to fund its Weapons of Mass Destruction (WMD) and ballistic missiles programs.

A. (U) TORNADO CASH Is an Entity that May Be Sanctioned under IEEPA

(U) As explained in *Sections IV.A – IV.B* below, **TORNADO CASH** is an entity that provides cryptocurrency mixing services through Tornado Cash and related smart contracts. Although **TORNADO CASH** purports to be only a decentralized software project, OFAC assesses that **TORNADO CASH** is an entity — that is, a "partnership, association, trust, joint venture, corporation, group, subgroup, or other organization," that may be designated pursuant to the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-1708 (IEEPA). *See* section 6(b), E.O. 13694, as amended; section 9(b), E.O. 13722. **TORNADO CASH**'s organizational structure consists of: (1) its founders — Alexey Pertsev, Roman Semenov, and Roman Storm — and other associated developers, who together launched the Tornado Cash mixing service, developed new Tornado Cash mixing service features, created the Tornado Cash Decentralized Autonomous Organization (DAO), and actively promote the platform's popularity in an attempt to increase is user base; and (2) the DAO, which is responsible for voting on and implementing new features created by the developers. In order to participate in the **TORNADO CASH** DAO, members must obtain "TORN," a virtual token issued by **TORNADO CASH** that gives the holder the right to vote on governance measures and influence the ongoing development and maintenance of the service operated by **TORNADO CASH**. Although TORN plays an important governance function, it is also a virtual currency that may be bought and sold

on secondary markets, the value of which increases as **TORNADO CASH** increases its user base and popularity. **TORNADO CASH** uses computer code known as "smart contracts" to implement its governance structure, provide mixing services, offer financial incentives for users, increase its user base, and facilitate the financial gain of its users and developers.

(U) One of the founders has claimed that **TORNADO CASH**'s use of decentralized blockchain governance makes it "technically impossible to enforce sanctions" against **TORNADO CASH**. In fact, the evidence available to OFAC shows that **TORNADO CASH**'s governance structure in many ways mimics common corporate structures: its founders and developers operate like a board of directors, while its DAO members operate like stockholders. These features allow **TORNADO CASH** to coordinate its operations and provide a valuable service to its users, which demonstrates that it is a sanctionable entity. If decentralized blockchain governance rendered a group like **TORNADO CASH** beyond the reach of IEEPA, then any number of malicious actors could easily launder the proceeds of cyber-enabled activities like the ***Sky Mavis-Ronin Bridge Heist***, merely by engaging in decentralized cryptocurrency mixing.

(U) Indeed, **TORNADO CASH** has taken concrete and coordinated steps to deploy, manage, promote, and profit from the Tornado Cash mixing service. **TORNADO CASH** has placed job advertisements. It has raised and maintained a community fund, from which it offers developers rewards for improving its code. **TORNADO CASH** has organized code deployment ceremonies, where a broader group of participants play a role in uploading changes of the service operated by **TORNADO CASH** to the Ethereum blockchain. It has refined its protocol to maximize anonymity and expand the kinds of transactions the service operated by **TORNADO CASH** can support. It has adopted qualifications and a compensation structure for "relayers," who facilitate withdrawals from the service operated by **TORNADO CASH**. Put simply, **TORNADO CASH** is more than an open-source software protocol. Since the launch of the service operated by **TORNADO CASH**, **TORNADO CASH** has operated in a coordinated fashion, taking concrete steps to enable its users to anonymize their transactions, whether licit or illicit. These actions, taken together, demonstrate that **TORNADO CASH** is an entity, as that term is defined by E.O. 13694, as amended, and E.O. 13722.

B. (U) **TORNADO CASH** Provides a Virtual Currency Mixing Service that Allows Users to Anonymously Transmit Virtual Currency

(U) As explained in *Section IV.C* below, the service operated by **TORNADO CASH** is designed to allow users to transact in virtual currencies while maintaining their anonymity. Because blockchain transactions are recorded in publicly available blocks, it is normally possible to trace a transaction to a user's identifiable virtual wallet. The service operated by **TORNADO CASH** attempts to address this privacy concern by allowing users to deposit virtual currencies in designated Tornado Cash virtual wallets, referred to as "anonymity pools." Each of these anonymity pools is a "smart contract," that is, a computer program running on the Ethereum blockchain that automatically executes a specified transaction at the request of Tornado Cash users. To use the service operated by **TORNADO CASH**, users deposit virtual assets in anonymity pools, where they are comingled with other Tornado Cash users' assets. Users then may withdraw their assets by presenting a cryptographic note proving their ownership. By comingling the assets of Tornado Cash users within an anonymity pool, it becomes difficult for

the public to connect any particular deposit with any particular withdrawal. To enhance the privacy-protecting function of the service operated by **TORNADO CASH** even further, users may employ a third-party relayer to conduct the withdrawal on behalf of the user. The relayer charges a fee to the user and pays a separate fee to **TORNADO CASH** based on terms set by the members of the **TORNADO CASH** DAO.

C. (U) **TORNADO CASH** Has a Property Interest in the Service Operated by **TORNADO CASH** and Has a Foreign Nexus

(U) **TORNADO CASH** has a property interest in the ongoing use of the service operated by **TORNADO CASH**. As explained in *Section IV.D* below, members of the **TORNADO CASH** DAO have received TORN tokens, a valuable virtual asset that can be bought and sold on secondary markets, in connection with the development, maintenance, and management of the service operated by **TORNADO CASH**. In turn, the **TORNADO CASH** DAO has authorized the payment of TORN rewards to developers who make improvements to the service operated by **TORNADO CASH**. And, as noted above, relayers must pay **TORNADO CASH** a fee for every transaction in which a relayer acts for a user of the service operated **TORNADO CASH**. Relayers are also required to acquire and set aside a specific number of TORN tokens, which can increase the value of TORN. **TORNADO CASH** thus has an interest in the ongoing use of the service operated by **TORNADO CASH**, which generates relayer fees for **TORNADO CASH** and contributes to the overall value of TORN tokens.

(U) As explained in *Section IV.E* below, OFAC assesses that foreign persons have a substantial interest in the service operated by **TORNADO CASH**. The founders of **TORNADO CASH** reside abroad. And based on publicly available information, a substantial share of TORN token holders are foreign persons. In addition, as noted above, DPRK cyber actors have used the service operated by **TORNADO CASH** to launder the proceeds of malicious cyber activities. Because of their early and substantial use of the service operated by **TORNADO CASH**, **TORNADO CASH** has distributed TORN tokens to such DPRK users. Those DPRK users thus have an ongoing stake in the service operated by **TORNADO CASH**.

(U) The basis of OFAC's action is set forth in *Section V.* below.

III. (U) IDENTIFYING INFORMATION

(U//~~FOUO~~) OFAC is providing the following identifiers to assist the public in identifying **TORNADO CASH** to assist in their sanctions compliance obligations, to include blocking property and interests in property of blocked persons.

1. (U) Name: **TORNADO CASH** [Exhibit 4, p. 1]
   (U) Website: Tornado.Cash [Exhibit 4, p. 1]
   (U) Organization Established Date: 2019 [Exhibit 120, p. 2]
   (U) Ether (ETH) Digital Currency Addresses (Smart Contracts):

(U) Tornado Cash Classic Contracts:

I. 0x12D66f87A04A9E220743712cE6d9bB1B5616B8Fc
II. 0x47CE0C6eD5B0Ce3d3A51fdb1C52DC66a7c3c2936
III. 0x910Cbd523D972eb0a6f4cAe4618aD62622b39DbF
IV. 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291
V. 0xD4B88Df4D29F5CedD6857912842cff3b20C8Cfa3
VI. 0xFD8610d20aA15b7B2E3Be39B396a1bC3516c7144
VII. 0x07687e702b410Fa43f4cB4Af7FA097918ffD2730
VIII. 0x23773E65ed146A459791799d01336DB287f25334
IX. 0x22aaA7720ddd5388A3c0A3333430953C68f1849b
X. 0x03893a7c7463AE47D46bc7f091665f1893656003
XI. 0x2717c5e28cf931547B621a5dddb772Ab6A35B701
XII. 0xD21be7248e0197Ee08E0c20D4a96DEBdaC3D20Af
XIII. 0x4736dCf1b7A3d580672CcE6E7c65cd5cc9cFBa9D
XIV. 0xd96f2B1c14Db8458374d9Aca76E26c3D18364307
XV. 0x169AD27A470D064DEDE56a2D3ff727986b15D52B
XVI. 0x0836222F2B2B24A3F36f98668Ed8F0B38D1a872f
XVII. 0x178169B423a011fff22B9e3F3abeA13414dDD0F1
XVIII. 0x610B717796ad172B316836AC95a2ffad065CeaB4
XIX. 0xbB93e510BbCD0B7beb5A853875f9eC60275CF498
XX. 0x84443CFd09A48AF6eF360C6976C5392aC5023a1F
XXI. 0xd47438C816c9E7f2E2888E060936a499Af9582b3
XXII. 0x330bdFADE01eE9bF63C209Ee33102DD334618e0a
XXIII. 0x1E34A77868E19A6647b1f2F47B51ed72dEDE95DD
XXIV. 0xdf231d99Ff8b6c6CBF4E9B9a945CBAcEF9339178
XXV. 0xaf4c0B70B2Ea9FB7487C7CbB37aDa259579fe040
XXVI. 0xa5C2254e4253490C54cef0a4347fddb8f75A4998
XXVII. 0xaf8d1839c3c67cf571aa74B5c12398d4901147B3
XXVIII. 0x6Bf694a291DF3FeC1f7e69701E3ab6c592435Ae7
XXIX. 0x3aac1cC67c2ec5Db4eA850957b967Ba153aD6279
XXX. 0x723B78e67497E85279CB204544566F4dC5d2acA0
XXXI. 0x0E3A09dDA6B20aFbB34aC7cD4A6881493f3E7bf7
XXXII. 0x76D85B4C0Fc497EeCc38902397aC608000A06607
XXXIII. 0xCC84179FFD19A1627E79F8648d09e095252Bc418
XXXIV. 0xD5d6f8D9e784d0e26222ad3834500801a68D027D
XXXV. 0x407CcEeaA7c95d2FE2250Bf9F2c105aA7AAFB512
XXXVI. 0x833481186f16Cece3f1Eeea1a694c42034c3a0dB
XXXVII. 0xd8D7DE3349ccaA0Fde6298fe6D7b7d0d34586193
XXXVIII. 0x8281Aa6795aDE17C8973e1aedcA380258Bc124F9
XXXIX. 0x57b2B8c82F065de8Ef5573f9730fC1449B403C9f
XL. 0x05E0b5B40B7b66098C2161A5EE11C5740A3A7C45
XLI. 0x23173fE8b96A4Ad8d2E17fB83EA5dcccdCa1Ae52
XLII. 0x538Ab61E8A9fc1b2f93b3dd9011d662d89bE6FE6
XLIII. 0x94Be88213a387E992Dd87DE56950a9aef34b9448
XLIV. 0x242654336ca2205714071898f67E254EB49ACdCe
XLV. 0x776198CCF446DFa168347089d7338879273172cF
XLVI. 0xeDC5d01286f99A066559F60a585406f3878a033e

(U) Tornado Cash Nova Contracts:

XLVII. 0xD692Fd2D0b2Fbd2e52CFa5B5b9424bC981C30696
XLVIII. 0xca0840578f57fe71599d29375e16783424023357
XLIX. 0xDF3A408c53E5078af6e8fb2A85088D46Ee09A61b
L. 0x743494b60097A2230018079c02fe21a7B687EAA5
LI. 0x94C92F096437ab9958fC0A37F09348f30389Ae79

(U) Governance Contracts:

LII. 0x5efda50f22d34F262c29268506C5Fa42cB56A1Ce
LIII. 0x2f50508a8a3d323b91336fa3ea6ae50e55f32185
LIV. 0xCEe71753C9820f063b38FDbE4cFDAf1d3D928A80
LV. 0xffbac21a641dcfe4552920138d90f3638b3c9fba
LVI. 0x179f48c78f57a3a78f0608cc9197b8972921d1d2
LVII. 0xb04E030140b30C27bcdfaafFFA98C57d80eDa7B4
LVIII. 0x77777feddddffc19ff86db637967013e6c6a116c
LIX. 0x3efa30704d2b8bbac821307230376556cf8cc39e
LX. 0x746aebc06d2ae31b71ac51429a19d54e797878e9

(U) Relayer Registry Contracts:

LXI. 0xd90e2f925DA726b50C4Ed8D0Fb90Ad053324F31b
LXII. 0x5f6c97C6AD7bdd0AE7E0Dd4ca33A4ED3fDabD4D7
LXIII. 0xf4B067dD14e95Bab89Be928c07Cb22E3c94E0DAA
LXIV. 0x58E8dCC13BE9780fC42E8723D8EaD4CF46943dF2
LXV. 0x01e2919679362dFBC9ee1644Ba9C6da6D6245BB1
LXVI. 0x2FC93484614a34f26F7970CBB94615bA109BB4bf
LXVII. 0x26903a5a198D571422b2b4EA08b56a37cbD68c89
LXVIII. 0xB20c66C4DE72433F3cE747b58B86830c459CA911
LXIX. 0x2573BAc39EBe2901B4389CD468F2872cF7767FAF

(U) Other Contracts:

LXX. 0x527653eA119F3E6a1F5BD18fbF4714081D7B31ce
LXXI. 0x653477c392c16b0765603074f157314Cc4f40c32
LXXII. 0x88fd245fEdeC4A936e700f9173454D1931B4C307
LXXIII. 0x09193888b3f38C82dEdfda55259A82C0E7De875E
LXXIV. 0x5cab7692D4E94096462119ab7bF57319726Eed2A
LXXV. 0x756C4628E57F7e7f8a459EC2752968360Cf4D1AA
LXXVI. 0x722122dF12D4e14e13Ac3b6895a86e84145b6967
LXXVII. 0x94A1B5CdB22c43faab4AbEb5c74999895464Ddaf
LXXVIII. 0xb541fc07bC7619fD4062A54d96268525cBC6FfEF
LXXIX. 0xD82ed8786D7c69DC7e052F7A542AB047971E73d2
LXXX. 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384 [Exhibit 177, pp. 1–9]
LXXXI. 0xF67721A2D8F736E75a49FdD7FAd2e31D8676542a
LXXXII. 0x9AD122c22B14202B4490eDAf288FDb3C7cb3ff5E
LXXXIII. 0xD691F27f38B395864Ea86CfC7253969B409c362d
LXXXIV. 0xaEaaC358560e11f52454D997AAFF2c5731B6f8a6

LXXXV. 0x1356c899D8C9467C7f71C195612F8A395aBf2f0a
LXXXVI. 0xA60C772958a3eD56c1F15dD055bA37AC8e523a0D
LXXXVII. 0xBA214C1c1928a32Bffe790263E38B4Af9bFCD659
LXXXVIII. 0xb1C8094B234DcE6e03f10a5b673c1d8C69739A00
LXXXIX. 0xF60dD140cFf0706bAE9Cd734Ac3ae76AD9eBC32A

[Exhibit 101, pp. 2–10]

(U) Ether (ETH) Digital Currency Addresses (Externally Owned Account):
I. 0x8589427373D6D84E98730D7795D8f6f8731FDA16

[Exhibit 195, p. 1]

IV. BACKGROUND

(U) This section summarizes and explains information necessary to understand **TORNADO CASH** and its operations.

- (U) Part A details key information related to virtual currencies, including key concepts, how Ethereum and similar blockchains function, and how cryptocurrency mixing services relate to the broader cryptocurrency ecosystem.
- (U) Part B details **TORNADO CASH** and key aspects of how this entity operates.
- (U) Part C details the Tornado Cash mixing service. Throughout this memorandum, OFAC will refer to the entity proposed for designation with the bold and capitalized "**TORNADO CASH**." OFAC will use "Tornado Cash" without bolding or capitalization when that term serves as a descriptor, such as in "the Tornado Cash smart contracts." When directly quoting from sources, OFAC retains the formatting used in the source. Some of the sources also refer to Tornado.Cash, which refers to the domain which hosted some of the resources associated with the entity and its services.
- (U) Part D describes **TORNADO CASH**'s property and interests in property.
- (U) Part E details the property interest of foreign persons in **TORNADO CASH**.

A. (U) *Virtual Currencies*

1. (U) *Virtual Currencies*: Key Concepts

a. (U) *Virtual Currencies: Blockchains and Tokens*

(U) According to an October 2020 U.S. Department of Justice Report of the Attorney General's Cyber-Digital Task Force (the "Cyber-Digital Task Force Report"), "virtual currency" is a digital representation of value that, like traditional coin and paper currency, functions as a medium of exchange—i.e., it can be digitally traded or transferred, and can be used for payment or investment purposes. Virtual currency is a type of "virtual asset" that is separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets. "Cryptocurrency" refers to a specific type of virtual currency with key characteristics. The vast majority of cryptocurrencies are decentralized, in that they lack a central administrator

to issue currency and maintain payment ledgers[4]—in other words, there is no central bank. Instead, cryptocurrencies rely on complex algorithms, a distributed ledger that is often referred to as the "blockchain," and a network of peer-to-peer[5] users to maintain an accurate system of payments and receipts. Some examples of cryptocurrencies include Bitcoin, Litecoin, and Ether. [Exhibit 179, pp. 14–15]

(U) According to the website of Crypto.com, "like crypto coins, crypto tokens are designed using blockchain technology; however, crypto tokens aren't native to a blockchain. Instead, they're built on top of it, often utilizing smart contracts[6] to fulfil a variety of purposes. While crypto coins mimic traditional currencies, crypto tokens are more like assets or even deeds. A crypto token can represent a share of ownership in a Decentralized Autonomous Organization (DAO),[7] a digital product or non-fungible token (NFT),[8] or even a physical object. Crypto tokens can be bought, sold, and traded like coins, but they aren't used as a medium of exchange. To use a real-world example, crypto tokens are more like coupons or vouchers, while crypto coins are like dollars and cents. There are numerous types of crypto tokens: Some governance tokens offer holders voting rights in a DAO. Certain tokens, known as "utility tokens" may provide access to certain services or products developed by the token issuer. Most crypto tokens are designed to be used within a blockchain project or decentralized app (or "dapp").[9] Unlike crypto coins, tokens are created and distributed by the project developer for the particular intended purpose or use of those tokens. Once tokens are in the hands of purchasers, they can be used in accordance with their design. For example, Axie Infinity, one of the best-known play-to-earn (P2E) [games] on the market, features a utility token called Smooth Love Potions (SLP). By earning or purchasing SLP, players can perform exclusive in-game tasks." [Exhibit 89, p. 4]

(U) According to the Cyber-Digital Task Force Report, cryptocurrency can be exchanged directly person to person; through a cryptocurrency exchange; or through other intermediaries. The storage of cryptocurrency is typically associated with an individual "wallet," which is similar to a virtual account. Wallets can interface with blockchains and generate and/or store the public keys (which are roughly akin to a bank account number) and private keys (which function like a PIN or password) that are used to send and receive cryptocurrency. [Exhibit 179, p. 15]

---

[4] (U) According to an October 2018 NIST report, a ledger is a record of transactions. [Exhibit 130, p. 63]
[5] (U) According to a May 17, 2022, Cointelegraph article, accessed on October 1, 2022, peer-to-peer (P2P) trading is a type of cryptocurrency exchange method that allows traders to trade directly with one another without the need for a centralized third party to facilitate the transactions. [Exhibit 152, p. 2] According to Cointelegraph's website, Cointelegraph was founded in 2013 and is the leading independent digital media resource covering a wide range of news on blockchain technology, crypto assets, and emerging fintech trends. [Exhibit 23, p. 1]
[6] (U) Smart contracts are further explained in *Section IV.A.2* (***Virtual Currencies*: Ethereum**) below.
[7] (U) According to the "Decentralized Autonomous Organizations" page of Ethereum's website, [redacted] a DAO is a Decentralized Autonomous Organization which is member-owned community without centralized leadership. [Exhibit 157, p. 1] DAOs will be explained in detail in *Section IV.B.2* (***TORNADO CASH*: Decentralized Autonomous Organization (DAO)**) below.
[8] (U) According to a Cointelegraph article, nonfungible tokens, or NFTs, are verifiably unique representations of digital and physical goods. Each NFT generally differs in makeup, and therefore likely differs in value as well. [Exhibit 115, p. 1]
[9] (U) Decentralized Apps are further described in *Section IV.A.2* (***Virtual Currencies*: Ethereum**) section below.

(U) According to a September 24, 2021, Council on Foreign Relations[10] report, cryptocurrency users send funds between digital wallet addresses. These transactions are then recorded into "blocks," and confirmed across the network. Blockchains do not record real names or physical addresses, only the transfers between digital wallets, and thus confer a degree of anonymity on users. However, if the identity of a wallet owner becomes known, their transactions can be traced. The prices of Bitcoin and many other cryptocurrencies vary based on global supply and demand. [Exhibit 110, pp. 1–2]

b. (U) *Virtual Currencies: Smart Contracts*

(U//~~FOUO~~) As described in *Section IV.B.2* (***TORNADO CASH*: Decentralized Autonomous Organization (DAO)**), **TORNADO CASH** uses smart contracts to implement its governance structure. As described below in *Section IV.C.2* (***The Tornado Cash Mixing Service*: How the Tornado Cash Smart Contracts Enable Mixing**), **TORNADO CASH** deployed smart contracts to multiple blockchains to operationalize its mixing service.

(U) According to the website of Ethereum, "Ethereum calls the programs uploaded to and executed by the network smart contracts. At a very basic level, you can think of a smart contract like a sort of vending machine: a script that, when called with certain parameters, performs some actions or computation if certain conditions are satisfied. For example, a simple vendor smart contract could create and assign ownership of a digital asset[11] if the caller sends ETH to a specific recipient. Because developers can write arbitrary executable applications into the Ethereum Virtual Machine[12] (EVM) by publishing smart contracts, these are often also called DApps, or Decentralized Apps." [Exhibit 103, pp. 4–6]

(U) According to a May 26, 2018 post on the website of the Harvard Law School Forum on Corporate Governance, "smart contracts" is a term used to describe computer code that automatically executes all or parts of an agreement and is stored on a blockchain-based platform. Before a compiled smart contract actually can be executed on certain blockchains, an additional step is required, namely, the payment of a transaction fee for the contract to be added to the chain and executed upon. In the case of the Ethereum blockchain, smart contracts are executed on the EVM, and this payment, made through the ether cryptocurrency, is known as "gas." The more complex the smart contract (based on the transaction steps to be performed), the more gas that must be paid to execute the smart contract. Thus, gas currently acts as an important gate to

---

[10] (U) According to its website, the Council on Foreign Relations is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries. Founded in 1921, CFR takes no institutional positions on matters of policy. [Exhibit 82, p. 7]

[11] (U) According to an October 2018 NIST report, a digital asset is any asset that is purely digital, or is a digital representation of a physical asset. [Exhibit 130, p. 62]

[12] (U) According to the website of Ethereum, [redacted] the Ethereum Virtual Machine is the global virtual computer whose state every par[redacted]work stores and agrees on. Any participant can request the execution of arbitrary code on the EVM; code execution changes the state of the EVM. [Exhibit 103, p. 5]

prevent overly complex or numerous smart contracts from overwhelming the EVM. [Exhibit 199, p. 1]

c. (U) *Virtual Currencies: Governance*

(U) According to an October 2018 National Institute of Science and Technology (NIST) report, the "governance" of blockchain networks refers to the rules, practices, and processes by which the blockchain network is directed and controlled. A common misconception is that blockchain networks are systems without control and ownership. This is not strictly true. Permissioned blockchain networks are generally set up and run by an owner or consortium, which governs the blockchain network. Permissionless blockchain networks are often governed by blockchain network users, publishing nodes,[13] and software developers. [Exhibit 130, p. 46]

(U) According to a June 27, 2022 blog post by Chainalysis,[14] Decentralized Autonomous Organizations (DAOs) are intended to provide a new, democratized management structure for businesses, projects, and communities, in which any member can vote on organizational decisions just by buying into the project. At a high level, this is how DAOs work:

1. DAO founders create a new cryptocurrency, known as a governance token;
2. They distribute these tokens to users, backers, and other stakeholders; and
3. Each token corresponds to a set amount of voting power within the organization. It also corresponds to a price on the secondary market, where it can be bought and sold at will.

[Exhibit 59, p. 1]

(U) According to Chainalysis, while this process is often described as a way to decentralize power, governance token data suggests that DAO ownership is highly concentrated. By analyzing the distribution of ten major DAOs' governance tokens, Chainalysis finds that, across several major DAOs, less than 1 percent of all holders have 90 percent of the voting power. This has meaningful implications for DAO governance. For example, if just a small portion of the top 1% of holders worked together, they could theoretically outvote the remaining 99% on any decision. This has obvious practical implications and, in terms of investor sentiment, likely affects whether small holders feel that they can meaningfully contribute to the proposal process. [Exhibit 59, pp. 1–2]

d. (U) *Virtual Currencies: DPRK Illicit Finance Risks*

(U) According to the U.S. Department of the Treasury's 2022 National Proliferation Financing Risk Assessment (NPFRA), the DPRK's malicious cyber activities are an important source of

---

[13] (U) According to NIST, a node is an individual system within a blockchain network: 1. Full Node — a node that stores the entire blockchain, ensures transactions are valid, a publishing node is a node that, in addition to all responsibilities required of a full node, is tasked with extending the blockchain by creating and publishing new blocks. Also known as mining node, committing node, minting node. 2. Lightweight Node — a node that does not store or maintain a copy of the blockchain and must pass their transactions to full nodes. [Exhibit 130, p. 14]

[14] (U) According to the "About Us" page of its website, [redacted] Chainalysis provides blockchain-related data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 60 countries. Their data powers investigations, compliance, and market intelligence software that has been used to solve some of the world's most high-profile criminal cases and grow consumer access to virtual currency safely. [Exhibit 26, p. 1]

revenue generation for its military budget. In April 2020, the Departments of State, the Treasury, Homeland Security, and Justice co-published a DPRK Cyber Threat Advisory that highlighted the DPRK's malicious cyber activities and how the DPRK has targeted financial institutions and other private sector actors to fulfill its foreign policy ends. These include (1) disrupting critical infrastructure; (2) targeting those critical of the regime; (3) engaging in cyber-enabled financial theft and money laundering; and (4) compromising computers and network systems to generate virtual assets (a technique known as "cryptojacking"). DPRK state-sponsored cyber actors are subordinate to the RECONNAISSANCE GENERAL BUREAU* (RGB*),[15] the DPRK's main intelligence agency and a UN- and U.S.-designated entity. [Exhibit 200, p. 9]

(U) According to the NPFRA, proliferation financing[16] networks are increasingly exploiting the digital economy, including by engaging in the systematic mining and trading of virtual assets and the hacking of virtual asset service providers (VASPs). The DPRK's capacity and willingness to engage in increasingly sophisticated malicious cyber activity, against both traditional financial institutions, such as central banks and private firms, and the virtual assets sector, have grown considerably since 2018. There is no evidence that a proliferation network has used a virtual asset to procure a specific proliferation-sensitive good or technology[17] as an input to a WMD or ballistic missile program. However, virtual assets play an essential role in revenue generation and moving assets across borders. States and groups that are involved in exploiting the digital economy for sanctions evasion have used existing virtual assets, like Bitcoin, Ether, XRP, and Litecoin, among others. Hackers affiliated with or linked to the DPRK have conducted a broad range of criminal cyber activity to "further the strategic and financial interests of the DPRK government and its leader, Kim Jong-un." In many cases, the activities directly target U.S. individuals and companies (including, but not limited to, financial institutions). In April 2020, the Departments of State, Homeland Security, and the Treasury, along with the FBI, released Guidance on the North Korean Cyber Threat to provide a comprehensive resource on how cyber actors linked to the DPRK threaten both "traditional" financial institutions as well as new financial technology companies, especially VASPs. Proliferation networks are increasingly embracing certain types of virtual assets that enhance user anonymity. This activity is a significant source of revenue raised in violation of U.S. and UN sanctions. [Exhibit 200, pp. 1, 29–30]

(U) As explained in detail in Exhibits 54, 65, and 114, to address the illicit finance risks posed by virtual currencies, the U.S. Department of the Treasury has designated multiple persons under its sanctions authorities:

---

[15] (U) On January 2, 2015, OFAC blocked the property and interests in property of the RECONNAISSANCE GENERAL BUREAU* (RGB*) pursuant to E.O. 13687, "Imposing Additional Sanctions With Respect To North Korea". [Exhibit 149, pp. 2–3] The RGB* was listed in the annex to E.O. 13551 of August 30, 2010, "Blocking Property of Certain Persons With Respect to North Korea." [Exhibit 2, p. 4]

[16] (U) According to the NPFRA, financing of proliferation refers to the risk of raising, moving, or making available funds, other assets or economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related material (including both dual-use technologies and dual-use goods for non-legitimate purposes). [Exhibit 200, p. 4]

[17] (U) Given the context of this exhibit, OFAC assesses that "proliferation sensitive good or technology" references goods or technology that can be used in the development of WMD, including dual-use technologies or related material.

- On September 21, 2021, the U.S. Department of the Treasury designated the virtual currency exchange Suex;
- On May 6, 2022, the U.S. Department of the Treasury designated the virtual currency mixer Blender.io;
- On November 8, 2021 the U.S. Department of the Treasury designated the virtual currency exchange Chatex; and
- On April 5, 2022 the U.S. Department of the Treasury designated the virtual currency exchange Garantex and the Darknet Market Hydra Market.

(U//~~FOUO~~) Summarizing the above, this section explained following core concepts necessary to understand **TORNADO CASH**:

- (U//~~FOUO~~) Blockchains are a form of distributed database that may record ownership of virtual assets that are known as virtual currencies or cryptocurrencies.
- (U//~~FOUO~~) Smart contracts are applications built on blockchain networks that execute specified tasks.
- (U//~~FOUO~~) Blockchains and smart contracts can be employed to enable new forms of governance and governance structures, such as Decentralized Autonomous Organizations.
- (U//~~FOUO~~) Decentralized Autonomous Organizations are blockchain-enabled management structures in which individuals who obtain tokens can vote on organizational decisions.
- (U//~~FOUO~~) Virtual currencies and blockchains have created new illicit finance vulnerabilities that have been exploited by threat actors.

2. (U) *Virtual Currencies*: Ethereum

(U//~~FOUO~~) As detailed in *Section IV.B* (***TORNADO CASH***), and *Section IV.C* (***The Tornado Cash Mixing Service***), Tornado Cash smart contracts have been deployed primarily on the Ethereum blockchain. This subsection provides additional background and defines terminology specific to Ethereum.

a. (U) *Ethereum: How Ethereum Works*

(U) According to the website of Ethereum, "transactions are cryptographically signed instructions from accounts. An account will initiate a transaction to update the state of the Ethereum network. The simplest transaction is transferring ETH from one account to another. An Ethereum transaction refers to an action initiated by an externally owned account, in other words an account managed by a human, not a contract. For example, if Bob sends Alice 1 ETH, Bob's account must be debited and Alice's must be credited. This state-changing action takes place within a transaction. Transactions, which change the state of the Ethereum Virtual Machine (EVM), need to be broadcast to the whole network. Any node can broadcast a request for a transaction to be executed on the EVM; after this happens, a validator[18] will execute the

[18] (U) According to the website of Ethereum, [redacted] it takes a 32 ETH [deposit] to activate validator software. As a validator you will be responsible for storing data, processing transactions, and adding new

transaction and propagate the resulting state change to the rest of the network. Transactions require a fee and must be included in a validated block Transaction Lifecycle. Once the transaction has been submitted the following happens:

- Once you send a transaction, cryptography generates a transaction hash.
- The transaction is then broadcast to the network and included in a pool with lots of other transactions.
- A validator must pick your transaction and include it in a block in order to verify the transaction and consider it "successful."
- As time passes, the block containing your transaction will be upgraded to "justified" then "finalized." These upgrades make it much more certain that your transaction was successful and will never be altered. Once a block is "finalized," it could only ever be changed by an attack that would cost many billions of dollars."

[Exhibit 107, pp. 1–2, 13]

(U) According to the website of Ethereum, Ether (ETH) is the native cryptocurrency of the Ethereum blockchain. Any participant who broadcasts a transaction request must also offer some amount of ETH to the network as a "bounty." The network will award this bounty to whoever eventually does the work of verifying the transaction, executing it, committing it to the blockchain, and broadcasting it to the network. The amount of ETH paid corresponds to the time required to do the computation. [Exhibit 103, p. 4]

(U) According to the website of Ethereum, an Ethereum account is an entity with an ETH balance that can send transactions on the Ethereum blockchain. Accounts can be user-controlled or deployed as smart contracts. There are two Ethereum account types: *externally owned*, or controlled by anyone with the corresponding private keys,[19] and a *smart contract*[20] deployed to the Ethereum protocol network and controlled by code. The key differences are:

- Externally owned:
  - Creating an account costs nothing;
  - Can initiate transactions;
  - Transactions between externally owned accounts can only be ETH/token transfers.
- Smart contract:
  - Creating a contract has a cost because you are using network storage;
  - Can only send transactions in response to receiving a transaction;
  - Transactions from an external account to a contract account can trigger code that can execute many different actions, such as transferring tokens or even creating a new contract. [Exhibit 58, pp. 1–2]

---

blocks to the blockchain. This will keep Ethereum secure for everyone and earn you new ETH in the process. [Exhibit 221, p. 2] OFAC assesses that anyone with 32 ETH can opt in to become a validator by taking 32 ETH

[19] (U//FOUO) [redacted] [Exhibit 27, p. 44]

[20] (U//FOUO) The exhibit refers to "contract" rather than "smart contract." Because these terms are used interchangeably in this exhibit, OFAC assesses that all Ethereum contracts referenced in this exhibit are smart contracts.

(U//~~FOUO~~) [redacted] [Exhibit 106, p. 6]

b. (U) *Ethereum: ERC-20 Tokens*

(U//~~FOUO~~) As will be described in *Section IV.B* (***TORNADO CASH***) and *Section IV.C* (***The Tornado Cash Mixing Service***), **TORNADO CASH** uses a token called TORN to manage its governance and distribute income derived from **TORNADO CASH**'s operations. **TORNADO CASH** created TORN (an ERC-20 token) as a smart contract deployed on the Ethereum blockchain contract.

(U) According to Investopedia, "ERC-20" refers to a scripting standard used within the Ethereum blockchain. This technical standard dictates a number of rules and actions that an Ethereum token or smart contract must follow and steps to be able to implement it. It is perhaps easiest to think of ERC-20 as a set of basic guidelines and functions that any new token created in the Ethereum network must follow. [Exhibit 21, p. 4]

3. (U) ***Virtual Currencies*: Mixing Services**

(U//~~FOUO~~) As will be described in *Section IV.B* (***TORNADO CASH***) and *Section IV.C* (***The Tornado Cash Mixing Service***), the purpose of **TORNADO CASH** and the Tornado Cash smart contracts is to provide a non-custodial[21] cryptocurrency mixing service.

(U) According to the Cyber-Digital Task Force Report, "mixers" and "tumblers"[22] are entities that attempt to obfuscate the source or owner of particular units of cryptocurrency by mixing the cryptocurrency of several users prior to delivery of the units to their ultimate destination. For a fee, a customer can send cryptocurrency to a specific address that is controlled by the mixer. The mixer then commingles this cryptocurrency with funds received from other customers before sending it to the requested recipient address. [Exhibit 179, p. 53]

(U) According to a February 18, 2022 blogpost on CERTIK's[23] website, one of the primary purposes of blockchain analysis is to trace the flow of funds between addresses. This may be to follow the proceeds of an exploit,[24] or to establish a transaction chain linking two or more

---

[21] (U) According to the website of Gemini, [redacted] with a non-custodial wallet, you have sole control of your private keys, which in turn control your cryptocurrency and prove the funds are yours. With a custodial wallet, another party controls your private keys. Most custodial wallets these days are web-based exchange wallets. [Exhibit 226, p. 1] According to its website, Gemini is a crypto exchange that is a New York trust company regulated by the New York State Department of Financial Services. [Exhibit 227, p. 2]

[22] (U//~~FOUO~~) OFAC uses the terms "mixer" and "tumbler" interchangeably in this memorandum.

[23] (U) According to its website, CERTIK is a pioneer in blockchain security, utilizing best-in-class Formal Verification and AI technology to secure and monitor blockchains, smart contracts, and Web3 apps. [Exhibit 109, p. 1]

[24] (U//~~FOUO~~) [redacted] [Exhibit 53, p. 15]

wallets. The immutability of blockchains makes the technology well-suited to establishing historical claims and chains of strong correlation. [Exhibit 108, p. 3]

(U) According to an August 23, 2022 blog post by Chainalysis, a cryptocurrency mixer is a service that blends the cryptocurrencies of many users together to obfuscate the origins and owners of the funds. Because Bitcoin, Ethereum, and most other public blockchains are transparent, this level of privacy is otherwise hard to achieve. Mixers collect, pool, and pseudo-randomly[25] shuffle the cryptocurrencies deposited by many users. Later, the funds are withdrawn to new addresses under the control of each user. [Exhibit 63, pp. 1–2]

(U) According to an August 23, 2022 blog post by Chainalysis, centralized custodial mixers, which emerged as early as 2011, temporarily take ownership of users' funds and are typically run by a single operator. Because this type of mixing service is both centralized and custodial, users face additional privacy risks. They are also often a target of law enforcement, as financial enforcement agencies treat them as unregistered money services businesses. [Exhibit 63, p. 3]

(U) According to an August 23, 2022 blog post by Chainalysis, smart contract mixers[26] are non-custodial and do not combine users' funds in just one transaction. Instead, the user sends their funds to the mixer, receives a cryptographic note proving that they are the depositor, and then, whenever they would like, sends the mixer that note to withdraw the funds to a new address. [Exhibit 63, p. 3]

a. (U) *Mixing Services: Illicit Uses*

(U) According to a July 14, 2022 blog post by Chainalysis, "crypto[currency] mixers are a go-to tool for cybercriminals on the blockchain. Chainalysis finds that in 2022, crypto addresses tied to illicit activity transferred nearly 10 percent of their funds to mixers — with no other address type sending more than 0.3 percent. Cryptocurrency mixers saw significant quarter-over-quarter volume increases starting in 2020 and continuing through 2021. While that growth has leveled off somewhat this year, it remains close to all-time highs. The increases come primarily from growth in the volume sent from centralized exchanges, DeFi[27] protocols, and most notably, addresses connected to illicit activity. Illicit addresses account for 23 percent of funds sent to mixers so far in 2022, up from 12 percent in 2021. What stands out most is the huge volume of funds moving to mixers from addresses associated with sanctioned entities, especially in Q2 2022. [Exhibit 116, pp. 1, 3–5]

(U) According to a February 2022 Chainalysis report, North Korean cybercriminals had a banner year in 2021, launching at least seven attacks on cryptocurrency platforms that extracted nearly

---

[25] (U) According to PCMag, pseudo-random numbers provide necessary values for processes that require randomness. It is called "pseudo" random, because the algorithm can repeat the sequence, and the numbers are thus not entirely random. [Exhibit 228, p. 1]

[26] (U//~~FOUO~~) As explained in *Sections IV.B* (***TORNADO CASH***) and *IV.C* (***The Tornado Cash Mixing Service***), **TORNADO CASH** provides smart contract mixing services.

[27] (U) According to Investopedia, Decentralized Finance (DeFi) is an emerging financial technology based on secure distributed ledgers similar to those used by cryptocurrencies. DeFi eliminates the fees that banks and other financial companies charge for using their services. Individuals hold money in a secure digital wallet, can transfer funds in minutes, and anyone with an internet connection can use DeFi. [Exhibit 203, p. 1]

$400 million worth of digital assets last year. These attacks targeted primarily investment firms and centralized exchanges, and made use of phishing[28] lures, code exploits, malware,[29] and advanced social engineering[30] to siphon funds out of these organizations' internet-connected "hot" wallets[31] into DPRK-controlled addresses. Once North Korea gained custody of the funds, they began a careful laundering process to cover up and cash out. This is especially true for APT 38, also known as "LAZARUS GROUP*,"[32] which is led by DPRK's primary intelligence agency, the U.S.- and UN-sanctioned RECONNAISSANCE GENERAL BUREAU*.[33] While Chainalysis will refer to the attackers as North Korean-linked hackers more generally, many of these attacks were carried out by the LAZARUS GROUP* in particular. LAZARUS GROUP* first gained notoriety from its Sony Pictures and WannaCry cyberattacks, but it has since concentrated its efforts on cryptocurrency crime — a strategy that has proven immensely profitable. From 2018 on, the group has stolen and laundered massive sums of virtual currencies every year, typically in excess of $200 million. The most successful individual hacks, one on KuCoin and another on an unnamed cryptocurrency exchange, each netted more than $250 million alone. And according to the UN Security Council, the revenue generated from these hacks goes to support North Korea's WMD and ballistic missile programs. [Exhibit 178, p. 114]

(U) According to the same Chainalysis report, in 2021, North Korean hacking activity was on the rise once again. From 2020 to 2021, the number of North Korean-linked hacks jumped from four to seven, and the value extracted from these hacks grew by 40 percent. Interestingly, in terms of dollar value, Bitcoin now accounts for less than one fourth of the cryptocurrencies stolen by DPRK. In 2021, only 20% of the stolen funds were Bitcoin, whereas 22 percent were either ERC-20 tokens or altcoins.[34] For the first time ever, ETH accounted for a majority of the

---

[28] (U//~~FOUO~~) [redacted] [Exhibit 53, p. 25]

[29] (U//~~FOUO~~) [redacted] [Exhibit 53, p. 21]

[30] (U//~~FOUO~~) [redacted] [Exhibit 53, p. 28]

[31] (U) According to Investopedia, [redacted] a hot wallet is a cryptocurrency wallet that is always connected to the internet and cryptocurrency network. Hot wallets are used to send and receive cryptocurrency, and they allow you to view how many tokens you have available to use. [Exhibit 47, p. 3]

[32] (U) On September 13, 2019, the Department of the Treasury identified the LAZARUS GROUP* as meeting the definition of the Government of North Korea as set forth in section 9(d) of Executive Order 13722 because it is an agency, instrumentality, or controlled entity of the Government of North Korea. [Exhibit 113, p. 1]

[33] (U) On January 2, 2015, OFAC blocked the property and interests in property of the RECONNAISSANCE GENERAL BUREAU* (RGB*) pursuant to E.O. 13687, "Imposing Additional Sanctions With Respect To North Korea". [Exhibit 149, pp. 2–3] RGB* was listed in the annex to E.O. 13551 of August 30, 2010. [Exhibit 2, p. 4]

[34] (U) According to Investopedia, altcoins are generally defined as all cryptocurrencies other than Bitcoin. However, some people consider altcoins to be all cryptocurrencies other than Bitcoin and Ethereum because most cryptocurrencies are forked from one of the two. [Exhibit 187, p. 4] According to the website of makeuseof.com, [redacted] the term "forking" has been used within the software development community for decades. At the inception of its usage, "forking" mainly referred to copying a piece of software and then developing it parallel to its trunk copy. But the term's meaning evolved over time and now defines a specific phenomenon in software development. Software is "forked" when a rift occurs within its developing team, which could be due to

funds stolen at 58 percent. The growing variety of cryptocurrencies stolen has necessarily increased the complexity of DPRK's cryptocurrency laundering operation. Today, DPRK's typical laundering process is as follows:

1. ERC-20 tokens and altcoins are swapped for ETH via decentralized exchange (DEX)
2. ETH is mixed
3. Mixed ETH is swapped for Bitcoin via DEX
4. Bitcoin is mixed
5. Mixed Bitcoin is consolidated into new wallets
6. Bitcoin is sent to deposit addresses at crypto-to-fiat exchanges based in Asia—potential cash-out points. [Exhibit 178, pp. 115–117]

(U) According to the same Chainalysis report, Chainalysis observed a massive increase in the use of mixers among DPRK-linked actors in 2021. More than 65 percent of DPRK's stolen funds were laundered through mixers this year, up from 42 percent in 2020 and 21 percent in 2019, suggesting that these threat actors have taken a more cautious approach with each passing year. The DPRK is a systematic money launderer, and their use of multiple mixers — software tools that pool and scramble cryptocurrencies from thousands of addresses — is a calculated attempt to obscure the origins of their ill-gotten cryptocurrencies while off ramping[35] into fiat. DeFi platforms like DEXs provide liquidity for a wide range of ERC-20 tokens and altcoins that may not otherwise be convertible into cash. When DPRK swaps these coins for ETH or BTC they become much more liquid, and a larger variety of mixers and exchanges become usable. Moreover, DeFi platforms do not take custody of user funds and many do not collect know-your-customer (KYC) information, meaning that cybercriminals can use these platforms without having their assets frozen or their identities exposed. [Exhibit 178, pp. 115–117]

(U) According to OFAC's Frequently Asked Question #561, published on OFAC's website on March 19, 2018, the United States' whole-of-government strategies to combat global threats such as terrorism, transnational organized crime, malicious cyber activity, narcotics trafficking, WMD proliferation, and human rights abuses include targeting an array of activities, including the use of digital currencies or other emerging payment systems to conduct proscribed financial transactions and evade U.S. sanctions. The strategies draw from a broad range of tools and authorities to respond to the growing and evolving threat posed by malicious actors using new payment mechanisms. OFAC will use sanctions in the fight against criminal and other malicious actors abusing digital currencies and emerging payment systems as a complement to existing tools, including diplomatic outreach and law enforcement authorities. To strengthen our efforts to combat the illicit use of digital currency transactions under our existing authorities, OFAC may include as identifiers on the SDN List specific digital currency addresses associated with blocked persons. [Exhibit 117, p. 2]

---

differences of opinion regarding the project's direction or personality clashes. A faction or member of the development team will then take the program's source code and start independent development under a different name, approach, and direction. Thus, even though a fork is based on its parent software's source code, it is a new and independent project in its own right. Because it is hard to legally secure the rights to a propriety software source code, forking occurs almost exclusively within the free software development world. This type of software's "open source" nature also means that any user is within their rights to use, study, change, and distribute both it and its source code. [Exhibit 78, p. 2]

[35] (U) According to an August 18, 2020 CoinTelegraph article accessed on October 3, 2020, crypto offramps are a way to convert your cryptocurrency into fiat [currency]. [Exhibit 193, p. 4]

B. (U) ***TORNADO CASH***

(U) As will be detailed below, **TORNADO CASH** is an entity[36, 37] that provides cryptocurrency mixing services. OFAC assesses that **TORNADO CASH** is an entity — that is, a "partnership, association, trust, joint venture, corporation, group, subgroup, or other organization" — that may be designated pursuant to the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-1708 (IEEPA). *See* section 6(b), E.O. 13694, as amended; section 9(b), E.O. 13722. **TORNADO CASH**'s organizational structure consists of: (1) its founders —– Alexey Pertsev, Roman Semenov, and Roman Storm — and other associated developers, who together launched the Tornado Cash mixing service, developed new Tornado Cash mixing service features, created the **TORNADO CASH** Decentralized Autonomous Organization (DAO), and actively promote the platform's popularity in an attempt to increase is user base; and (2) the DAO, which is responsible for voting on and implementing new features created by the developers. In order to participate in the **TORNADO CASH** DAO, members must obtain "TORN," a virtual token issued by **TORNADO CASH** that gives the holder the right to vote on governance measures and influence the ongoing development and maintenance of the service operated by **TORNADO CASH**. Although TORN plays an important governance function, it is also a virtual currency that may be bought and sold on secondary markets, the value of which increases as **TORNADO CASH** increases its user base and popularity. **TORNADO CASH** uses computer code known as "smart contracts" to implement its governance structure, provide mixing services, offer financial incentives for users, increase its user base, and facilitate the financial gain of its users and developers.

(U//~~FOUO~~) **TORNADO CASH** collects fees through its "relayers," which provide a widely used, anonymity-enhancing service for users. In order for a relayer to be listed on the Tornado Cash relayer registry, the relayer must "stake" (i.e., deposit) TORN, the **TORNADO CASH** DAO's governance token. **TORNADO CASH** collects a fee from relayers for each transaction processed by the relayer, and distributes those fees to members of the **TORNADO CASH** DAO. The relayers, in turn, collect a fee from users of **TORNADO CASH**.

(U//~~FOUO~~) Specifically, an Ethereum transaction processed by **TORNADO CASH** through a relayer involves several fees:

1. The Ethereum "gas" fee, which is the fee paid in Ethereum by the initiator of any transaction on the Ethereum network to the validators who process the transactions.
2. The fee paid by the Tornado Cash user to the relayer, which is deducted from the funds deposited by the user to the Tornado Cash smart contract. In the case of an Ethereum transaction, this fee would be paid in Ethereum.
3. The fee paid by the relayer to **TORNADO CASH**, which is paid in TORN and deducted from the TORN that the relayer staked to be listed as an available relayer by **TORNADO CASH**. These TORN fees are distributed to members of the DAO who have staked their TORN to vote on **TORNADO CASH** governance proposals. This voting process is

[36] (U) E.O. 13694, as amended, defines an entity as a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization. [Exhibit 99, p. 2]
[37] (U) E.O. 13722 defines an entity as a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization. [Exhibit 100, p. 5]

further described in *Section IV.B.2*, (***TORNADO CASH:* Decentralized Autonomous Organization (DAO)**).

(U//~~FOUO~~) Relayers are more fully described in *Section IV.C.4 (**The Tornado Cash Mixing Service*: The Relayer Network).**

1. (U) ***TORNADO CASH*: Founders and Developers**

(U [redacted]

[Exhibit 3, p. 1]

(U) According to a January 25, 2022 CoinDesk article, in an interview with CoinDesk, Tornado Cash co-founder Roman Semenov said, "The Tornado Cash team mostly does research and publishes the code to GitHub.[38, 39] All the deployments, protocol changes, and important decisions are made by the community via Tornado Governance Decentralized Autonomous Organization and deployment ceremonies," which are events when new code is pushed live. [Exhibit 6, pp. 3–4]

(U) According to the employment opportunity page on **TORNADO CASH**'s website, [redacted] **TORNADO CASH** had an open job advertisement that states that it is "looking for a Solidity[40] Engineer, to join our ranks and strengthen our skill set." The advertisement states that hires will:

- Design and write smart contracts on Ethereum to implement new features;
- Collaborate and share experiences with an enthusiastic and driven team;
- Contribute integrating state-of-the-art features for the next version of the protocol;
- Work in a fast-paced and challenging environment;
- Be able to work autonomously, great communication remotely, and continually get self-connected; and

[38] (U) According to its website, [redacted] GitHub offers free and paid products for storing and collaborating on code. Some products apply only to personal accounts, while other plans apply only to organization and enterprise accounts. [Exhibit 80, p. 1]

[39] According to the website of the General Services Administration, accessed on October 24, 2022, GitHub is a web-based interface that uses Git, the open-source version control software that lets multiple people make separate changes to web pages at the same time. GitHub allows multiple developers to work on a single project at the same time, reduces the risk of duplicative or conflicting work, and can help decrease production time. With GitHub, developers can build code, track changes, and innovate solutions to problems that might arise during the site development process simultaneously. Non-developers can also use it to create, edit, and update website content. [Exhibit 219, pp. 1–2]

[40] (U) According to an article on Ethereum's website, last updated on February 15, 2022, Solidity is a programming language for implementing smart contracts. [Exhibit 118, p. 1]

- If interested, gain significant knowledge on zk-SNARKs[41] and improve your skills on this topic." [Exhibit 119, p. 1]

(U) According to an August 15, 2022 Cointelegraph article, in 2021, **TORNADO CASH** created a fund to provide incentives to key contributors to the project.[42] [Exhibit 18, pp. 1–2]

(U) According to the GitHub page of the archived code base of the software used by **TORNADO CASH**, the source code contains 34 different repositories.[43] [Exhibit 48, p. 1]

(U) According to the commit log for the "Tornado Core" repository, the most recent commit[44] was by user "Alexey Pertsev" on March 24, 2022. Another commit was by user "Roman Semenov" on October 31, 2021. Still another commit was by user "poma"[45] on October 29, 2021. [Exhibit 74, p. 1] OFAC assesses that the usernames "Alexey Pertsev" and "Roman Semenov" are associated with **TORNADO CASH** developers Alexey Pertsev and Roman Semenov. Additional information regarding these individuals is discussed in *Section IV.E.2.*

(U//~~FOUO~~) Based on the above information regarding the "Tornado Core" commit log, OFAC concludes that the software used and developed by **TORNADO CASH** has undergone active development by a core group of developers over a period of multiple years.

2. (U) *TORNADO CASH*: Decentralized Autonomous Organization (DAO)

[41] (U) According to the "What are zk-SNARKs?" page of the Zcash website, [redacted] "zk-SNARK" stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge," and refers to a proof of construction where one can prove possession of certain information, e.g. a secret key, without revealing that information, and without any interaction between the prover and verifier. [Exhibit 133, p. 1]

[42] (U) According to the August 15, 2022 Cointelegraph article, accessed on August 25, 2022, "the fund was held in a community-managed multi-signature wallet with five peer-elected members validating transactions who were selected because of their contributions to the project. Following the United States' sanctioning of USD Coin (USDC) and Ethereum addresses associated with the crypto mixer Tornado Cash, the signatories of the projects' multi-signature community fund have disbanded." "However, given that interacting with Tornado Cash now comes with more risks — including penalties for U.S. citizens ranging from fines of up to $10 million to prison time of up to 30 years — the community members in charge of the fund have vacated their posts and handed control to the project's DAO. On August 12, the signatories started to relinquish their ability to manage the fund. On August 12, [2022], the signatories started to relinquish their ability to manage the fund. And on August 14, 2022 all five members of the multi-signature wallet completely removed their access, leaving only the governance wallet as the fund's sole owner." [Exhibit 18, p. 2]

[43] (U) According to the website of GitHub, [redacted] a repository is usually used to organize a single project. Repositories can contain folders and files, images, videos, spreadsheets, and data sets, anything your project needs. Often, repositories include a README file, a file with information about your project. [Exhibit 229, p. 2]

[44] (U) According to the website of GitHub, you can save small groups of meaningful changes as *commits*. Similar to saving a file that has been edited, a *commit* records changes to one or more files in your branch. [Exhibit 80, p. 1]

[45] (U//~~FOUO~~) A GitHub user profile page for "poma" [redacted] links to the **TORNADO CASH** website and lists the user's real name as "Roman Semenov." [Exhibit 208, p. 1] Based on this information, OFAC assesses that the username "poma" was also controlled by **TORNADO CASH** founder Roman Semenov.

(U) **TORNADO CASH** is controlled by a DAO, which is comprised of members who have obtained TORN[46] tokens. TORN tokens provide members of the DAO with ownership stake in a fashion similar to stockholders; the more TORN tokens a member has, the more voting power they have. Developers of **TORNADO CASH** research and develop new features to **TORNADO CASH** and post them on websites such as GitHub for members of the DAO to propose to the collective members of the DAO for implementation. If a vote to implement passes, the DAO implements the new features in a process called Trusted Setup Ceremony. The DAO is the central controlling mechanism of **TORNADO CASH**.

a. (U) *The TORN Token*

(U) **TORNADO CASH** governance is accomplished through the DAO, which is made up of individuals who have been issued TORN tokens. According to a September 6, 2021 blog post on the website of Medium,[47] authored by **TORNADO CASH**, which has since been deleted by the author, and which was accessed by OFAC through the Wayback Machine's August 8, 2022 archive, the blog post describes the **TORNADO CASH** decision making processes, which combines both on-chain[48] and off-chain[49] governance:

> "Governance is at the heart of every decentralized protocol and Tornado Cash does not deviate from this rule. By principle, for a decentralized protocol to function correctly, the decision-making process needs to be put between the hands of its users. Those users form a community that has the right & duty to shape the next versions of the tool they use. Usually, this community has the means to express itself through governance tokens. In other words, if the protocol was the community's battlefield, governance would be its weapon & tokens its ammunition. For the DAO to run smoothly, governance rules need to be clearly specified and cover all potential areas. We just need to take a look at political voting systems around the world to assert that decision making rules have a tremendous impact on the final made decision. On-chain governance offers the community (i.e., TORN holders) the means to implement the desired changes to their protocol. If the community agrees on adding or changing a given feature, the update will only be implemented if the on-chain governance rules are complied with. All those changes must go through proposals. Those proposals can be suggested to Tornado Cash users & TORN holders directly on https://app.tornado.cash/governance [the Tornado Cash Website], by any eligible community [i.e., DAO] member." [Exhibit 70, pp. 2–4]

---

[46] (U) According to an August 13, 2022 Bitcoin.com article, TORN is the Tornado Cash governance token with a fixed supply, and which may be used to propose changes to Tornado Cash and its governance, and vote on such changes. There are approximately 1,511,065 TORN tokens, with 30 percent reserved for the developers and contributors. [Exhibit 34, p. 1]

[47] (U) According to the "About" page of its website, accessed on April 22, 2022, Medium is an open platform where over 100 million readers come to find insightful and dynamic thinking, where expert and undiscovered voices alike dive into the heart of any topic. [Exhibit 41, p. 1]

[48] (U) According to an October 2018 NIST report, "on-chain" refers to data that is stored or a process that is implemented and executed within a blockchain system. [Exhibit 189, p. 82]

[49] (U) According to an October 2018 NIST report, "off-chain" refers to data that is stored or a process that is implemented and executed outside of any blockchain system. [Exhibit 189, p. 82]

(U) According to the website[50, 51] of **TORNADO CASH** written by the "Tornado Team" and accessed through the Wayback Machine's June 17, 2022 archive, TORN is an ERC-20-compatible token with a fixed supply that governs **TORNADO CASH**. TORN holders can make proposals and vote to change the protocol via governance. **TORNADO CASH** asserts that TORN is not a fundraising device or investment opportunity. It also indicates that the initial distribution of TORN was broken down as follows:

- 5% (500,000 TORN): Airdrop[52] to early users of Tornado Cash ETH pools;[53]
- 10% (1,000,000 TORN): Anonymity mining[54] for Tornado Cash ETH pools, distributed linearly over one year;
- 55% (5,500,000 TORN): DAO treasury,[55] will be unlocked linearly over five years with three-month cliff;[56]
- 30% (3,000,000 TORN): Founding developers and early supporters, will be unlocked linearly over three years with one year cliff. [Exhibit 4, p. 1]

[50] (U) Following OFAC's August 8, 2022 designation of **TORNADO CASH**, the website "Tornado.Cash" was shut down and is no longer accessible, except through the Internet Archive.

[51] (U) According to its website, the Internet Archive, a 501(c)(3) non-profit, is building a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, it provides free access to researchers, historians, scholars, people with print disabilities, and the general public. Its mission is to provide "Universal Access to All Knowledge." [Exhibit 20, p. 1]

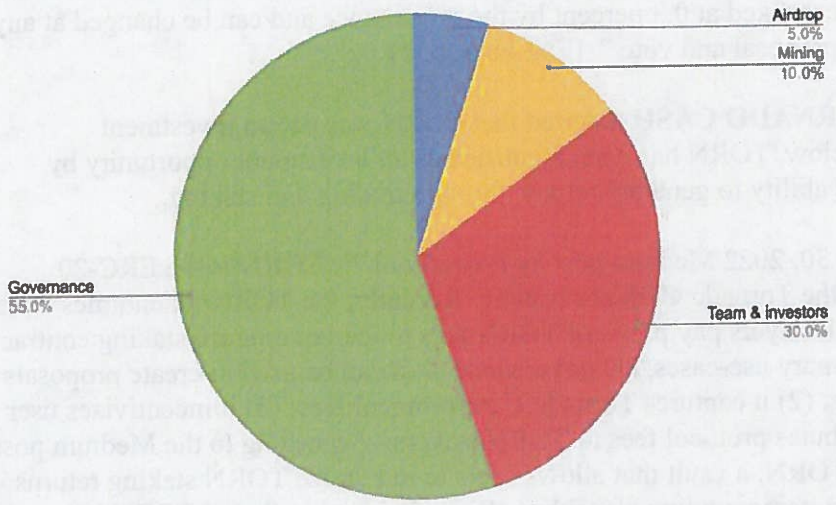
[52] (U) According to Cointelegraph, airdrops are a marketing strategy used by startups to give tokens to existing cryptocurrency traders for free or in exchange for minimal promotional work. [Exhibit 22, p. 1]

[53] (U//~~FOUO~~) Based on the context in which the term is used in this exhibit, OFAC assesses that "pools" refers to liquidity pools. According to a June 7, 2022 CoinDesk article, a liquidity pool is a digital pile of cryptocurrency locked in a smart contract. This results in creating liquidity for faster transactions. [Exhibit 220, p. 2]

[54] (U) Anonymity Mining is explained in more detail in *Section IV.C.3* (***The Tornado Cash Mixing Service*: Anonymity Mining**).

[55] (U) The DAO Treasury is explained in more detail in *Section IV.B.2.b* (***TORNADO CASH*: Decentralized Autonomous Organization (DAO)**)

[56] (U) According to a December 9, 2021 post on Medium, cliffs are known as the period of time that must pass before the release of tokens starts. The duration of the cliffs can vary depending on the purpose of an allocation. Methods like cliffs (also known as "lock-up" periods) and vesting emerge as a means of aligning the interests of all participants and earning the trust of investors. [Exhibit 69, pp. 1–2]



[Exhibit 4, pp. 1–2]

(U) According to **TORNADO CASH's** website, accessed through the Wayback Machine's April 20, 2022 archive, "since its inception, the TORN token has been used by Tornado Cash users for governance. Its main utility is to allow the suggestion of proposals and voting both on-chain (through locked TORN for governance proposals) and off-chain (on Snapshot).[57] Since the execution of Tornado Cash's tenth governance proposal, TORN token[s] ha[ve] gained one other useful utility. Indeed, with the introduction of a decentralized relayer register, a staking[58] reward has been implemented for all holders with locked TORN in the governance contract. TORN holders can still lock their tokens into the governance contract as they used to for governance purposes. The significant difference is that they are now able to receive a portion of the fees collected by the protocol from relayers. Obviously, the proportion of the reward will be equal to the proportion of their locked TORN. The collection of these fees was made possible by the implementation of a decentralized relayer registry. To be listed on the protocol user interface (UI),[59] relayers need to stake a given amount of TORN (currently set by governance at 300 TORN) and keep enough TORN locked (~40 TORN at the moment in April 2022) to be able to pay back the transaction fee to the staking contract. In a nutshell, for each withdrawal through

---

[57] (U) Snapshot is a centralized voting system. It provides flexibility on how voting power is calculated for a vote. Snapshot supports various voting option types to cater the needs of organizations. Creating proposals and voting on Snapshots is user-friendly and does not cost gas as the process is performed off-chain. [Exhibit 67, p. 1]

[58] (U) According to Cointelegraph, staking refers to a strategy where one can invest in a stake pool with a fraction of the number of tokens required to become a validator on a blockchain, while the staking pool rewards users on a daily, weekly or quarterly basis, depending on the cryptocurrency being staked. [Exhibit 25, p. 4] Staking Pools allow people to join other crypto investors to raise staking capital. Participants can then deposit any amount of tokens to a staking pool and start earning passive income proportional to the amount on their holdings. [Exhibit 49, p. 3]

[59] (U) According to the website of TechTarget, UI is the point of human-computer interaction and communication in a device. [Exhibit 16, p. 1]

the relayer method, the chosen relayer has to pay a fee to the protocol[60] from the staked balance. Currently,[61] this fee has been fixed at 0.3 percent by the governance and can be changed at any time through an on-chain proposal and vote." [Exhibit 5, p. 1]

(U//~~FOUO~~) Although **TORNADO CASH** asserted that TORN was not an investment opportunity, as detailed below, TORN has been identified as an investment opportunity by multiple sources due to its ability to generate returns through trading and staking.

(U) According to an April 30, 2022 Medium post by PowerPool,[62] "TORN is the ERC-20 governance token used in the Tornado Cash ecosystem. Recently, the TORN tokenomics[63] were updated, and now, TORN Relayers pay protocol TORN fees to the governance staking contract. Thus, TORN has three primary use-cases, (1) governance — it can be used to create proposals and to participate in voting; (2) it captures Tornado.Cash protocol fees; (3) it incentivizes user participation since it distributes protocol fees to TORN stakers. According to the Medium post, PowerPool announced ppTORN, a vault that allows users to maximize TORN staking returns thanks to PowerPool's auto-compounding algorithm. PowerPool states that ppTORN is a smart contract that aggregates user deposits into the Tornado Cash governance staking contract. The ppTorn vault harvests and auto-compounds TORN rewards (protocol fees); ppTORN uses a smart algorithm for harvesting and re-staking which allows it to compound the rewards for Tornado token holders while reducing overall gas costs." [Exhibit 143, pp. 1–3]

(U) According to a February 9, 2021 BTC Geek[64] article, **TORNADO CASH** "has been in operation for a while now and has proven its effectiveness in real-world adversarial scenarios. To that end, the protocol has come up with its own token, TORN. This is currently a governance-only token but it is not hard to see how it can become a value capture token via fees. The users of [**TORNADO CASH**] would not mind paying some fees for peace of mind and privacy. TORN's tokenomics is well thought out and the inflation schedule is very gradual with no bumpy lockups expiring. In addition, there are no pesky VCs[65] in TORN's allocation ready to dump on retail as soon as possible and bring down its value. The allocation of TORN has been very fair, providing TORN to early users of the Tornado protocol and using TORN as an

---

[60] (U//~~FOUO~~) Based on the context in which this information is presented, OFAC assesses that "protocol," as used in this context, is a reference to the Tornado Cash Governance Contract.
[61] (U//~~FOUO~~) Given that April 2022 is referenced previously in this exhibit, OFAC assesses that "currently," as used here, refers to on or about April 2022.
[62] (U) According to the Medium post, PowerPool DAO manages a growing range of structured DeFi products. PowerPool DAO's mission is to create and actively manage a broadly diversified portfolio of automated, gas/capital-efficient, structured DeFi product portfolios deployed across EVM-compatible networks, with 100% of management fees accruing to the xCVP stakers controlling the DAO. [Exhibit 143, p. 3]
[63] (U) According to CoinDesk, tokenomics is a catch-all for the elements that make a particular cryptocurrency valuable and interesting to investors. That includes everything from a token's supply and how it's issued to things like what utility it has. [Exhibit 1, p. 2]
[64] (U) According to its website, BTC Geek is a blog and journalistic resource that caters to the Bitcoin and crypto community and publishes everything from news to opinion. [Exhibit 12, p. 1]
[65] (U//~~FOUO~~) According to Cointelegraph, the crypto industry is maturing fast, with many quick to compare it to the gold rush. And with industry maturity, users are beginning to witness a flood of traditional and retail investors flocking to the crypto space. Venture capital funds and other institutional investors are increasingly eyeing cryptocurrency businesses to see if there's a profit to be made in financing them. [Exhibit 188, p. 1] OFAC assesses "VC," as used here, is a reference to venture capital.

incentive mechanism to increase the number of users and total value locked (TVL)[66] in the protocol. This is essential to the success of TORN and Tornado since the larger the anonymity set, the better it is for the users. You can also farm[67] TORN instead of buying TORN from an exchange. This is a long-term play since the amount of TORN that you earn depends on the time you are staked. However, this is good because TORN is gradually released into the market." [Exhibit 142, pp. 1–3]

(U) According to a May 11, 2022 article on the website of AltCoinBuzz,[68] DeFi earnings platform PowerPool has announced a new vault for the Tornado Cash token, TORN. The protocol made the announcement that the ppTORN pool was live on May 10, 2022. According to the announcement, the team calculated that during a two-month period, users generated 61 percent APY[69] in the ppTORN vault. This is better than the 52 percent they earned for direct staking without the vault. There was almost $100,000 in total value locked in the vault at the time of writing. [Exhibit 144, pp. 1–2]

(U) According to a March 5, 2022 Crypto News Australia[70] article, TORN surged 94 percent following the launch of its latest network updates. The latest price action for TORN follows the adoption and implementation of the protocol's tenth on-chain governance proposal, which saw the addition of relayers to the network. The community voted overwhelmingly in favor of the proposal, which was accepted on February 19, 2022. Following the launch of the relayers on March 2, 2022. The price of TORN spiked from around $37 to around the $67 mark. [Exhibit 176, pp. 2–3]

(U) According to a January 25, 2022 CoinDesk article, in an interview with CoinDesk, **TORNADO CASH** co-founder Roman Semenov said, "The Tornado Cash team mostly does research and publishes the code to GitHub. All the deployments, protocol changes, and important decisions are made by the community via Tornado Governance[71] [DAO] and deployment ceremonies," an event when new code is pushed live. [Exhibit 6, pp. 3–4]

(U) According to the "FAQ" page of **TORNADO CASH**'s website [redacted] "the governance of Tornado Cash is completely decentralized, controlled, and governed by its

---

[66] (U) According to a January 27, 2022 CoinDesk article, TVL is the overall value of crypto assets deposited in a DeFi protocol or in DeFi protocols generally. It has emerged as a key metric for gauging interest in that particular sector of the crypto industry. TVL includes all the coins deposited in all of the functions that DeFi protocols offer, including staking, lending, and liquidity pools. [Exhibit 173, p. 2]

[67] (U//~~FOUO~~) OFAC assesses that this is a reference to Anonymity Mining.

[68] (U) According to its website, AltCoinBuzz is an independent digital media outlet that delivers the latest news and opinions in the world of Cryptocurrencies, Blockchain Technology, Regulations, Adoption and Blockchain Gaming. [Exhibit 40, p. 1]

[69] (U) According to the website of CoinMarketCap, APY is the rate of return gained over the course of a year on a specific investment. [Exhibit 105, p. 1]

[70] (U) According to its website, Crypto News was founded in 2017 as an online publication where readers can find independent news in relation to cryptocurrencies and blockchain. [Exhibit 172, p. 1]

[71] (U//~~FOUO~~) According to a page on the website of Ethereum titled "Introduction to Ethereum governance," *governance* is the systems in place that allow decisions to be made: "In a typical organizational structure, the executive team or a board of directors may have the final say in decision-making. Or perhaps shareholders vote on proposals to enact change. In a political system, elected officials may enact legislation that attempts to represent their constituents' desires. [Exhibit 50, p. 1]

DAO. By acquiring TORN tokens, customers can participate by voting on governance proposals." [Exhibit 160, p. 2]

(U) According to an August 12, 2022 Decrypt[72] article, the Tornado Cash TORN token is used by the Tornado Cash DAO to manage governance and voting. [Exhibit 7, p. 2]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's August 5, 2022 archive, thanks to the TORN token, protocol parameters and token distribution are completely under the community's control. [Exhibit 120, p. 3]

(U) According to the same September 6, 2021 Medium post, authored by "Tornado Cash," "to sum-up Tornado Cash governance rules:

- TORN tokens need to be locked[73] in the Tornado Cash governance contract to get used for governance & cannot be unlocked until the end of the proposal;
- A minimum of 1,000 locked TORN is needed to create a proposal on the [Tornado Cash app];
- Community members have a time-lapse of 3 days to vote with their locked TORN; A proposal is executed if:
  - (i) a 25,000 TORN quorum is reached, [and]
  - (ii) the number of TORN vouching for the proposal exceeds the number of TORN that are against it;
- Changes agreed on through those governance rules are binding, which means that any user can deploy them after a two-days time-lock and within a period of 3 days." [Exhibit 70, pp. 3–4]

(U) According to the same September 6, 2021 blog post on the website of Medium, on-chain governance helps maintain transparency as rules are clearly specified and known by the whole community. "It also enables changes and updates to get implemented in a decentralized environment where users are the actual stakeholders of the protocol. When the power lies in the hands of many individuals, decision making rules are crucial. This is especially true since those binding changes are directly deployed on the Blockchain and impact the functioning of the whole protocol. A wise man once said: with great power comes great responsibility. However, all decisions made by the community don't need to go through strict on-chain governance guidelines, locked tokens in contracts and Tornado Cash proposals system. Indeed, proposals can only concern specific areas such as changing reward parameters for Anonymity Points or changing certain core mining contracts. A lot of decisions, such as the use of the Tornado Cash Community Fund or the election of its multi-signature key holders, are made through off-chain governance."[74] [Exhibit 70, p. 4]

---

[72] (U) According to its website, Decrypt was founded in 2018 with a simple mission: to demystify the decentralized web. [Exhibit 196, p. 1]

[73] (U) According to the website of Binance, [redacted] the term token lockup refers to a specific period of time in which cryptocurrency tokens cannot be transacted or traded. Typically, these lockups are used as a preventive strategy to maintain a stable long-term value of a particular asset. [Exhibit 194, p. 1]

[74] (U) According to the encyclopedia section of the website of PCMag, accessed on October 24, 2022, off-chain governance is a blockchain that operates like any organization, wherein a core group of people make decisions. For

(U) According to a February 9, 2021 Coin Telegraph article, "[DeFi] 'stimulus checks' keep coming as Tornado Cash joins Uniswap, Badger DAO, StakeDAO, and others in "airdropping" a now-tradable TORN governance token to early protocol participants. Tornado Cash, which is an Ethereum "tumbling" service that obscures transactional history in order to preserve user privacy (as well as allow scammers and hackers a method to launder their funds), first announced the launch of a governance token in December. A snapshot for the airdrop was taken for Ethereum block 11400000, which was mined on December 6th, 2020[75] and addresses which had interacted with the protocol prior to that point were entitled to an amount of TORN tokens weighted to the frequency and amount of Ether they used. At current valuations, the distribution was one of the most lucrative for recipients to date. According to a post on community forums, the average recipient received 66.54 TORN tokens currently worth over $23,000, and the median user took in 21.24 tokens, worth $7500. The single largest recipient harvested over 2500 tokens worth a whopping $888,000. The 500,000 airdropped tokens represent just 5 percent of the eventual 10,000,000 total TORN supply." [Exhibit 121, pp. 1–2]

b. (U) Community Fund

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's June 17, 2022 archive, in June 2021, "to help build future enhanced versions of Tornado Cash, all skills and talents are well welcomed. Involvement opportunities are almost unlimited. Those opportunities involve any function or contribution that improves the protocol and its position within the blockchain ecosystem. The Tornado Cash community is looking for:

- Developers that can help continue building the protocol and its tools;
- Auditors who can review code to find bugs and vulnerabilities;
- Content creators in order to make educational or promotional content to attract new users to the protocol (videos, blogs, memes, etc.); and
- Potential hires for the DAO." [Exhibit 122, p. 1]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's June 17, 2022 archive, "in June 2021, [the] Tornado.Cash community[76] has voted the implementation of a community fund to reward its key contributors. The management of this fund lies with the community. Tornado.Cash users are the ones who decide whose contribution is eligible for a compensation. Tornado.Cash Community Fund has been allocated 5% of total available TORN of the governance treasury, broken down as follows:

- 5% of the already vested 485,300 TORN at that time, resulting on an initial transfer of 22.9 thousand TORN.

---

example, Bitcoin and Ethereum use off-chain governance. In contrast, on-chain governance is how a DAO operates. DAOs issue governance tokens, and members have voting rights because they purchased or were given voting tokens. [Exhibit 223, p. 1] According to its website, accessed on October 25, 2022, PCMagazine delivers lab-based, independent reviews of the latest products and services. [Exhibit 224, p. 1]

[75] (U) According to the website of Etherscan, [redacted] Ethereum block 11400000 occurred on December 6, 2020. [Exhibit 201, p. 1]

[76] (U//~~FOUO~~) Based on additional context provided in Exhibit 122, OFAC assesses that management of the community fund has included both control by the DAO and control by individuals selected to represent **TORNADO CASH**.

- 5% of the monthly 91,600 [TORN] that will be vested in the next 12 months, which result on a monthly transfer of approximately 4,600 TORN." [Exhibit 122, p. 2]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's June 17, 2022 archive, the monthly allocation of the Fund was programmed through Sablier, a protocol build on Ethereum that allows a live stream of remaining TORNs (second by second) over 12 months. In total, an amount of approximately 78,000 TORN was allocated to this Community Fund. As of the end of August 2021, the balance of the Community Fund is about 12,600 TORN vested in Sablier and 15,500 TORN in the gnosis safe. As of the beginning of 2022, the Community Fund (on Gnosis Safe) balance amounts to 36,400 TORN. Tornado.Cash Community Contract is 0xb04E030140b30C27bcdfaafFFA98C57d80eDa7B4. Funds are handled through a Multi-signature Wallet on Gnosis Safe. Keys to manage this wallet were put between the hand of 5 peer-elected community members. To validate a transaction, a consensus of 4-of-5 signatures is needed. Those multi-signatures key holders were chosen for their contribution & commitment to Tornado.Cash and its Community. They pledged to sign off transaction[s] following the community instructions. Those guidelines are expressed through forum discussion and corroborated by a Snapshot vote. All signers also pledged to resign if they no longer fulfill their allegiance to Tornado's prosperity. They can also be dismissed from their role under the decision of the community. To reward their commitment as signers & key contributors for Tornado.Cash community, a minimum of 100 TORN per month per signer has been deployed through Sablier. The current 5 multi-signatures key holders are:

- 0xd26BaA5F41CC7839CEdb020b6d98E1C6e1642D75
- 0x7c09bCa28ba3DB1CF7cd793696B161261cAC27b5
- 0x339B45fBEed1ab46Fe9c11f484b0Ea7220e75300
- 0x647e9e26DA82C29AAFbbFB1C3f45d916AA9b300d
- 0xEA27752f7D6687CB3Be2F180B997713b784c9911 [Exhibit 122, pp. 2–3]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's June 17, 2022 archive, "multi-signature wallet, members of the community have "the ability to ask the community for compensation from this fund to reward his/her contribution to Tornado.Cash. Each member also has the ability to request compensation on behalf of another member to reward him/her for his/her work. To this extent, a new category titled «Funding» has been created on [the] Tornado.Cash discussion forum. By creating a new post in the category, all members can open a funding request to use the Community Fund. Discussions regarding terms and conditions of such a request are discussed on this post. Once these terms and conditions are fixed, a vote is conducted on Snapshot to validate (or not) such a funding request." [Exhibit 122, p. 3]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's June 17, 2022 archive, "each specific funding request is accompanied by a Snapshot vote, where TORN holders can explicitly express their position. In order to vote on Snapshot, the community member needs to:

- Connect the wallet holding TORNs using MetaMask, WalletConnect, or Torus;
- Cast the vote, by either clicking on Accept or Refuse; and
- Confirm the vote." [Exhibit 122, pp. 4–6]

(U) According to an August 12, 2022 Theblock.co article, accessed November 5, 2022, "the Tornado Cash DAO community has voted in favor of adding the DAO's governance as a signatory to the treasury's multi-signatory (multisig) wallet. The Treasury looks after about $21.6 million across three different wallets. This vote began on Wednesday, based on a proposal on the Tornado Cash DAO governance page, and ended today with 100% approval from all 12 participants. These 12 participants contributed 51,000 TORN tokens to push the vote to completion. The voting process was hastily put together with the SnapShot initiated together with the proposal. Usually, there is a delay between a proposal being filed and the commencement on-chain. This lag is to create adequate time for the community to discuss the matter at hand. But it would have taken too long for the DAO. "As it is very important, we need to move fast on this subject. I will make a snapshot vote today so you guys can vote on it during 3 days," said the Tornado Cash DAO member who filed the proposal. With the vote passed, the DAO's treasury will now become a four-of-six multisig instead of the previous four-of-five multi-sig arrangement. The Tornado Cash DAO governance will now be added as a signatory to the treasury wallet. Multisig wallets require a specific minimum number of signatories to approve a transaction. In this case, four out of the six signers must approve any transaction from the treasury. In practice, this means that if the core developers want to make a transaction involving the treasury, they will need to get signatures from at least four of the six multisig holders. Since one of these holders is now the DAO, they may need to ask the DAO to approve a signature. This would require the DAO to vote on whether to do so." [Exhibit 204, pp. 1–3]

3. (U) *TORNADO CASH*: Smart Contracts Associated with TORNADO CASH

(U) According to an August 25, 2022 Coin Center article, each Tornado Cash pool is a smart contract deployed to Ethereum. Like other smart contracts, the pool contracts extend the functionality of Ethereum with specific operations that can be executed by any user of Ethereum according to the rules defined in the Tornado Cash contracts' code. [Exhibit 62, p. 6]

(U//~~FOUO~~) According to the website of **TORNADO CASH**, accessed by the Wayback Machine's June 17, 2022 archive, the Tornado Cash smart contracts include Tornado Cash Classic Pools Contracts,[77] Tornado Cash Nova Pool Contracts, Governance Contracts, Relayer Registry, and Other Contracts.[78] The smart contracts are as follows:

(U) Tornado Cash Classic Contracts:

I. 0x12D66f87A04A9E220743712cE6d9bB1B5616B8Fc
   - Name: 0.1 ETH Pool Contract

II. 0x47CE0C6eD5B0Ce3d3A51fdb1C52DC66a7c3c2936
   - Name: 1 ETH Pool Contract

III. 0x910Cbd523D972eb0a6f4cAe4618aD62622b39DbF

[77] (U) Each Tornado Cash pool takes deposits of a specific amount of a specific cryptocurrency.

[78] (U//~~FOUO~~) Although OFAC assesses that these smart contract addresses are associated with **TORNADO CASH**, OFAC was unable to confirm the accuracy of the labels assigned to the smart contracts by the **TORNADO CASH** website.

- Name: 10 ETH Pool Contract

IV. 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291
- Name: 100 ETH Pool Contract

V. 0xD4B88Df4D29F5CedD6857912842cff3b20C8Cfa3
- Name: 100 DAI[79] Pool Contract

VI. 0xFD8610d20aA15b7B2E3Be39B396a1bC3516c7144
- Name: 1,000 DAI Pool Contract

VII. 0x07687e702b410Fa43f4cB4Af7FA097918ffD2730
- Name: 10,000 DAI Pool Contract

VIII. 0x23773E65ed146A459791799d01336DB287f25334
- Name: 100,000 DAI Pool Contract

IX. 0x22aaA7720ddd5388A3c0A3333430953C68f1849b
- Name: 5,000 cDAI[80] Pool Contract

X. 0x03893a7c7463AE47D46bc7f091665f1893656003
- Name: 50,000 cDAI Pool Contract

XI. 0x2717c5e28cf931547B621a5dddb772Ab6A35B701
- Name: 500,000 cDAI Pool Contract

XII. 0xD21be7248e0197Ee08E0c20D4a96DEBdaC3D20Af
- Name: 5,000,000 cDAI Pool Contract

XIII. 0x4736dCf1b7A3d580672CcE6E7c65cd5cc9cFBa9D
- Name: 100 USDC[81] Pool Contract

XIV. 0xd96f2B1c14Db8458374d9Aca76E26c3D18364307
- Name: 1,000 USDC Pool Contract

XV. 0x169AD27A470D064DEDE56a2D3ff727986b15D52B
- Name: 100 USDT Pool Contract

XVI. 0x0836222F2B2B24A3F36f98668Ed8F0B38D1a872f
- Name: 1,000 USDT Pool Contract

XVII. 0x178169B423a011fff22B9e3F3abeA13414dDD0F1
- Name: 0.1 WBTC Pool Contract

XVIII. 0x610B717796ad172B316836AC95a2ffad065CeaB4
- Name: 1 WBTC Pool Contract

XIX. 0xbB93e510BbCD0B7beb5A853875f9eC60275CF498
- Name: 10 WBTC Pool Contract

---

[79] (U) According to the Blockchain Council, DAI is the first stable cryptocurrency that is decentralized and collateralized. It aims at reducing the volatility of trading on the blockchain. It is an ERC-20 token that ensures maintaining a value equal to one U.S dollar. [Exhibit 51, p. 3]

[80] (U) According to a Decrypt article from April 20, 2020, cDAI is a Compound protocol token, which is a system of openly accessible smart contracts built on Ethereum. Compound focuses on allowing borrowers to take out loans and lenders to provide loans by locking their crypto assets into the protocol called cTokens. New cTokens are created whenever a user deposits crypto-assets into the Compound protocol. If users want to take out a loan using ETH as collateral, they automatically receive cETH in return for their deposited ETH. Anyone can mint or create cTokens using an Ethereum wallet such as MetaMask, Coinbase wallet, or Huobi wallet plus one of the crypto assets the Compound system currently accepts. As of December 2019, users of Compound could borrow or lend BAT, DAI, ETH, REP, USDC, WBTC, and ZRX. [Exhibit 52, p. 2]

[81] (U) According to Investopedia, USD Coin (USDC) is a digital currency that is fully backed by U.S. dollar assets. USDC is a tokenized U.S. dollar, with the value of one USDC coin pegged 1:1 to the value of one U.S. dollar. The value of USDC is designed to remain stable, making USDC a stablecoin. [Exhibit 73, p. 1]

XX. 0x84443CFd09A48AF6eF360C6976C5392aC5023a1F
- Name: 0.1 ETH Pool Contract

XXI. 0xd47438C816c9E7f2E2888E060936a499Af9582b3
- Name: 1 ETH Pool Contract

XXII. 0x330bdFADE01eE9bF63C209Ee33102DD334618e0a
- Name: 10 ETH Pool Contract

XXIII. 0x1E34A77868E19A6647b1f2F47B51ed72dEDE95DD
- Name: 100 ETH Pool Contract

XXIV. 0xdf231d99Ff8b6c6CBF4E9B9a945CBAcEF9339178
- Name: 1,000 xDAI[82] Pool Contract

XXV. 0xaf4c0B70B2Ea9FB7487C7CbB37aDa259579fe040
- Name: 10,000 xDAI Pool Contract

XXVI. 0xa5C2254e4253490C54cef0a4347fddb8f75A4998
- Name: 100,000 xDAI Pool Contract

XXVII. 0xaf8d1839c3c67cf571aa74B5c12398d4901147B3
- Name: 500 AVAX[83] Pool Contract

XXVIII. 0x6Bf694a291DF3FeC1f7e69701E3ab6c592435Ae7
- Name: 0.1 ETH Pool Contract

XXIX. 0x3aac1cC67c2ec5Db4eA850957b967Ba153aD6279
- Name: 1 ETH Pool Contract

XXX. 0x723B78e67497E85279CB204544566F4dC5d2acA0
- Name: 10 ETH Pool Contract

XXXI. 0x0E3A09dDA6B20aFbB34aC7cD4A6881493f3E7bf7
- Name: 100 ETH Pool Contract

XXXII. 0x76D85B4C0Fc497EeCc38902397aC608000A06607
- Name: 100 DAI Pool Contract

XXXIII. 0xCC84179FFD19A1627E79F8648d09e095252Bc418
- Name: 1,000 DAI Pool Contract

XXXIV. 0xD5d6f8D9e784d0e26222ad3834500801a68D027D
- Name: 10,000 DAI Pool Contract

XXXV. 0x407CcEeaA7c95d2FE2250Bf9F2c105aA7AAFB512
- Name: 100,000 cDAI Pool Contract

XXXVI. 0x833481186f16Cece3f1Eeea1a694c42034c3a0dB
- Name: 5,000 cDAI Pool Contract

XXXVII. 0xd8D7DE3349ccaA0Fde6298fe6D7b7d0d34586193
- Name: 50,000 cDAI Pool Contract

XXXVIII. 0x8281Aa6795aDE17C8973e1aedcA380258Bc124F9
- Name: 500,000 cDAI Pool Contract

XXXIX. 0x57b2B8c82F065de8Ef5573f9730fC1449B403C9f
- Name: 5,000,000 cDAI Pool Contract

---

[82] (U) According to a March 3, 2021 Medium article, the xDai chain is an Ethereum-based sidechain that uses a Proof-of-Stake mechanism. It has been live since late 2018 and uses a stablecoin, xDai, as its native cryptocurrency. [Exhibit 75, p. 1]

[83] (U) According to a September 16, 2022 Forbes article, Avalanche (AVAX) is a cryptocurrency and blockchain platform set up to rival Ethereum. Within the Avalanche blockchain, AVAX is used as the token to support a suite of blockchain projects, such as tracking smart contracts. [Exhibit 85, p. 2]

XL. 0x05E0b5B40B7b66098C2161A5EE11C5740A3A7C45
- Name: 100 USDC Pool Contract

XLI. 0x23173fE8b96A4Ad8d2E17fB83EA5dcccdCa1Ae52
- Name: 1,000 USDC Pool Contract

XLII. 0x538Ab61E8A9fc1b2f93b3dd9011d662d89bE6FE6
- Name: 100 USDT[84] Pool Contract

XLIII. 0x94Be88213a387E992Dd87DE56950a9aef34b9448
- Name: 1,000 USDT Pool Contract

XLIV. 0x242654336ca2205714071898f67E254EB49ACdCe
- Name: 0.1 WBTC[85] Pool Contract

XLV. 0x776198CCF446DFa168347089d7338879273172cF
- Name: 1 WBTC Pool Contract

XLVI. 0xeDC5d01286f99A066559F60a585406f3878a033e
- Name: 10 WBTC Pool Contract

(U) Tornado Cash Nova Contracts:

XLVII. 0xD692Fd2D0b2Fbd2e52CFa5B5b9424bC981C30696
- Name: Tornado Pool

XLVIII. 0xca0840578f57fe71599d29375e16783424023357[86]
- Name: L1 Omnibridge Helper

XLIX. 0xDF3A408c53E5078af6e8fb2A85088D46Ee09A61b
- Name: Verifier 2

L. 0x743494b60097A2230018079c02fe21a7B687EAA5
- Name: Verifier 16

LI. 0x94C92F096437ab9958fC0A37F09348f30389Ae79
- Hasher / Poseidon 2

(U) Governance Contracts:

LII. 0x5efda50f22d34F262c29268506C5Fa42cB56A1Ce
- Name: Governance Contract

LIII. 0x2f50508a8a3d323b91336fa3ea6ae50e55f32185
- Name: Governance Vault (For Locked TORN)

LIV. 0xCEe71753C9820f063b38FDbE4cFDAf1d3D928A80
- Name: Deployer Contract

LV. 0xffbac21a641dcfe4552920138d90f3638b3c9fba
- Name: Governance Impl

LVI. 0x179f48c78f57a3a78f0608cc9197b8972921d1d2
- Name: Governance Vesting

---

[84] (U) According to Investopedia, Tether (USDT) is a cryptocurrency stablecoin pegged to the U.S. dollar and backed "100% by Tether's reserves." [Exhibit 102, p. 1]

[85] (U) According to a May 17, 2022 Decrypt article, WBTC stands for Wrapped Bitcoin, an ERC-20 token that represents Bitcoin—one WBTC equals one BTC. A BTC can be converted into a WBTC and vice-versa. Being an ERC-20 token makes the transfer of WBTC faster than normal Bitcoin, but the key advantage of WBTC is its integration into the world of Ethereum wallets, decentralized apps (DApps), and smart contracts. [Exhibit 76, p. 2]

[86] (U) According to Coin Center, this smart contract allows users to designate deposited ETH to be bridged to a Tornado Cash pool located on the Gnosis Chain blockchain. [Exhibit 62, pp. 24–25]

LVII. 0xb04E030140b30C27bcdfaafFFA98C57d80eDa7B4
- Name: Community Fund

LVIII. 0x77777feddddffc19ff86db637967013e6c6a116c
- Name: TORN Token

LIX. 0x3efa30704d2b8bbac821307230376556cf8cc39e
- Name: Voucher TORN Token

LX. 0x746aebc06d2ae31b71ac51429a19d54e797878e9
- Name: Mining v2

(U) Relayer Registry Contracts:

LXI. 0xd90e2f925DA726b50C4Ed8D0Fb90Ad053324F31b[87]
- Name: Tornado Router

LXII. 0x5f6c97C6AD7bdd0AE7E0Dd4ca33A4ED3fDabD4D7
- Name: Proxy of Fee Manager Contract

LXIII. 0xf4B067dD14e95Bab89Be928c07Cb22E3c94E0DAA
- Name: FeeManager

LXIV. 0x58E8dCC13BE9780fC42E8723D8EaD4CF46943dF2[88]
- Name: Proxy of Relayer Registry Contract

LXV. 0x01e2919679362dFBC9ee1644Ba9C6da6D6245BB1
- Name: Relayer Registry

LXVI. 0x2FC93484614a34f26F7970CBB94615bA109BB4bf
- Name: Proxy of Staking Contract

LXVII. 0x26903a5a198D571422b2b4EA08b56a37cbD68c89
- Name: Tornado Staking Rewards

LXVIII. 0xB20c66C4DE72433F3cE747b58B86830c459CA911
- Name: Proxy of Instance Registry Contract

LXIX. 0x2573BAc39EBe2901B4389CD468F2872cF7767FAF
- Name: Instance Registry

(U) Other Contracts:

LXX. 0x527653eA119F3E6a1F5BD18fbF4714081D7B31ce[89]
- Name: Tornado.Cash Trees

LXXI. 0x653477c392c16b0765603074f157314Cc4f40c32
- Name: Tree Update Verifier

LXXII. 0x88fd245fEdeC4A936e700f9173454D1931B4C307
- Name: Reward Verifier

LXXIII. 0x09193888b3f38C82dEdfda55259A82C0E7De875E
- Name: Withdraw Verifier

LXXIV. 0x5cab7692D4E94096462119ab7bF57319726Eed2A
- Name: Reward Swap

---

[87] (U) According to Coin Center, this smart contract maintains a list of Tornado Cash pools, which can be used by users to route deposits and withdrawals to the correct Tornado Cash pool. [Exhibit 62, p. 24]
[88] (U) According to Coin Center, this smart contract allows anyone to register as a Tornado Cash Relayer. [Exhibit 62, p. 24]
[89] (U) According to Coin Center, this smart contract holds a merkle tree (a kind of list) of all Tornado Cash deposit and withdrawal events. [Exhibit 62, p. 24]

LXXV. 0x756C4628E57F7e7f8a459EC2752968360Cf4D1AA
- Name: Echoer

LXXVI. 0x722122dF12D4e14e13Ac3b6895a86e84145b6967[90]
- Name: Proxy

LXXVII. 0x94A1B5CdB22c43faab4AbEb5c74999895464Ddaf[91]
- Name: Mixer 1

LXXVIII. 0xb541fc07bC7619fD4062A54d96268525cBC6FfEF[92]
- Name: Mixer 2

LXXIX. 0xD82ed8786D7c69DC7e052F7A542AB047971E73d2
- Name: Poseidon 3

LXXX. 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384[93]
- Name: Gitcoin Grants [Exhibit 177, pp. 1–9]

(U//~~FOUO~~) Etherscan[94] attributes the below smart contracts to **TORNADO CASH**. In addition, these smart contracts were deployed by address 0x8589427373D6D84E98730D7795D8f6f8731FDA16, which **TORNADO CASH** identified[95] as its donation address. Based on this, OFAC assesses that these addresses are associated with **TORNADO CASH:**

I. 0xF67721A2D8F736E75a49FdD7FAd2e31D8676542a
- Name: Tornado.Cash: 10,000 USDT [Pool Contract]
- Contract Creator: Tornado.Cash: Donate (0x8589427373D6D84E98730D7795D8f6f8731FDA16)

II. 0x9AD122c22B14202B4490eDAf288FDb3C7cb3ff5E
- Name: Tornado.Cash: 100,000 USDT [Pool Contract]
- Contract Creator: Tornado.Cash: Donate (0x8589427373D6D84E98730D7795D8f6f8731FDA16)

III. 0xD691F27f38B395864Ea86CfC7253969B409c362d
- Name: Tornado.Cash 10,000 USDC [Pool Contract]
- Contract Creator: Tornado.Cash: Donate (0x8589427373D6D84E98730D7795D8f6f8731FDA16)

IV. 0xaEaaC358560e11f52454D997AAFF2c5731B6f8a6
- Name: Tornado.Cash: 5,000 cUSDC [Pool Contract]
- Contract Creator: Tornado.Cash: Donate (0x8589427373D6D84E98730D7795D8f6f8731FDA16)

V. 0x1356c899D8C9467C7f71C195612F8A395aBf2f0a
- Name: Tornado.Cash: 50,000 cUSDC [Pool Contract]

---

[90] (U) According to Coin Center, this smart contract is an old version of Tornado.Cash: Router. [Exhibit 62, p. 25]
[91] (U) According to Coin Center, this smart contract is an old version of the Tornado Cash pools. [Exhibit 62, p. 26]
[92] (U) According to Coin Center, this smart contract is an old version of the Tornado Cash pools. [Exhibit 62, p. 26]
[93] (U) According to Coin Center, this smart contract is used to receive software development grants from the Gitcoin crowdfunding platform. [Exhibit 62, p. 31]
[94] (U) According to its website, EtherScan is the leading BlockChain explorer, search, API, and Analytics Platform for Ethereum. [Exhibit 29, p. 1]
[95] (U) On August 23, 2019, **TORNADO CASH** tweeted: "Now you can donate to any Ethereum project anonymously. Just withdraw your note to donation address. Try it out with Tornado Cash donation address 0x8589427373D6D84E98730D7795D8f6f8731FDA16." [Exhibit 195, p. 1]

- Contract Creator: Tornado.Cash: Donate (0x8589427373D6D84E98730D7795D8f6f8731FDA16)

VI. 0xA60C772958a3eD56c1F15dD055bA37AC8e523a0D
- Name: Tornado.Cash: 500,000 cUSDC [Pool Contract]
- Contract Creator: Tornado.Cash: Donate (0x8589427373D6D84E98730D7795D8f6f8731FDA16)

VII. 0xBA214C1c1928a32Bffe790263E38B4Af9bFCD659
- Name: Tornado.Cash: 50,000 cDAI [Pool Contract]
- Contract Creator: Tornado.Cash: Donate (0x8589427373D6D84E98730D7795D8f6f8731FDA16)

VIII. 0xb1C8094B234DcE6e03f10a5b673c1d8C69739A00
- Name: Tornado.Cash: 500,000 cDAI [Pool Contract]
- Contract Creator: Tornado.Cash Donate: (0x8589427373D6D84E98730D7795D8f6f8731FDA16)

IX. 0xF60dD140cFf0706bAE9Cd734Ac3ae76AD9eBC32A
- Name: Tornado.Cash: 10,000 DAI [Pool Contract]
- Contract Creator: Tornado.Cash: Donate (0x8589427373D6D84E98730D7795D8f6f8731FDA16)

[Exhibit 101, pp. 2–10]

(U) According to the website of Immunefi,[96] accessed through the Wayback Machine's May 27, 2022 archive, **TORNADO CASH** had a bug bounty program[97] which was focused on its smart contracts and was focused on preventing:

- Thefts or freezing of funds in anonymity pools
- Thefts or freezing of unclaimed yield (TORN anonymity mining)
- Theft of governance funds (Main on-chain Tornado DAO treasury only)
- On chain governance activity disruption. [Exhibit 175, p. 2]

(U) According to the website of Immunefi, accessed through the Wayback Machine's May 27, 2022 archive, the Tornado Cash bug bounty program has fixed rewards in TORN. The maximum reward is capped at 32,500 TORN, which was the equivalent of $1,300,000 at the time. [Exhibit 175, p. 3]

(U) According to the website of Immunefi, accessed through the Wayback Machine's May 27, 2022 archive, the following Tornado Cash smart contracts were in-scope for the Tornado Cash bug bounty program: 0.1 ETH pool, 1 ETH pool, 10 ETH pool, 100 ETH pool, 100 DAI pool, 1,000 DAI pool, 10,000 DAI pool, 100,000 DAI pool, 5,000 cDAI pool, 50,000 Cdai pool, 500,000 cDAI pool, 5,000,000 cDAI pool, 100 USDC pool, 1,000 USDC pool, 100

[96] (U) According to ImmuneFi's website, [redacted] founder and CEO Mitchell Amador launched Immunefi on December 9, 2020, as a bug bounty platform focused on web3 and smart contract security with the goal of making web3 safe for everyone. Immunefi provides bug bounty hosting, consultation, and program management services to blockchain and smart contract projects. [Exhibit 19, p. 1]

[97] (U) According to ImmuneFi's website, [redacted] bug bounty programs are open invitations to security researchers to discover and responsibly disclose vulnerabilities in projects' smart contracts and applications, which can save web3 projects hundreds of millions — and even billions — of dollars. For their good work, security researchers receive a reward based on the severity of the vulnerability. [Exhibit 19, p. 2]

USDT pool, 1,000 USDT pool, 0.1 WBTC, 1 WBTC, 10 WBTC, TORN Token, Governance Proxy, Reward Verifier, Withdraw Verifier, Tree Update Verifier, Reward Swap, TornadoCash Proxy, TornadoTrees, Miner, and Poseidon Hasher. [Exhibit 175, pp. 5–12]

(U//~~FOUO~~) Based on the above description of the **TORNADO CASH** bug bounty program, OFAC assesses that **TORNADO CASH** offered TORN that it controlled to help identify and remediate security vulnerabilities in the Tornado Cash smart contracts. The substantial value of the rewards offered by the bug bounty program demonstrates that **TORNADO CASH** believed that bugs in these smart contracts had the potential to cause damage to **TORNADO CASH**.

4. (U) ***TORNADO CASH*: Trusted Setup Ceremony**

(U//~~FOUO~~) As detailed below, **TORNADO CASH** has facilitated community involvement in deployment of smart contracts through a Trusted Setup Ceremony; OFAC assesses that these ceremonies increase the profile and privacy bona fides of **TORNADO CASH**, thus increasing its appeal to users. The involvement of large numbers of participants in such a ceremony distinguishes a smart contract that has undergone the ceremony from one that has not. Trusted Setup Ceremonies also demonstrate **TORNADO CASH**'s role in serving as a coordinating mechanism for an online community of users and supporters who might otherwise be unable to organize joint action to implement a smart contract-based mixing service.

(U) According to a May 2020 blog post on the Medium website, authored by "Tornado Cash," **TORNADO CASH** was "happy to announce that the Tornado Cash Trusted Setup Ceremony has been launched." Tornado Cash "ask[ed the] crypto community to help make Tornado Cash fully trustless by contributing to the ceremony." Tornado Cash explained: "We plan to end the ceremony on May 10, 2020. If there is high demand, we will keep it open for a couple more days. [Exhibit 39, pp. 1–3]

(U) According to the website of Vitalik Buterin, one of the founders of Ethereum, a trusted setup ceremony is a procedure that is done once to generate a piece of data that must then be used every time some cryptographic protocol is run. Generating this data requires some secret information; the "trust" comes from the fact that some person or some group of people has to generate these secrets, use them to generate the data, and then publish the data and forget the secrets. But once the data is generated, and the secrets are forgotten, no further participation from the creators of the ceremony is required. [Exhibit 55, p. 1]

(U//~~FOUO~~) According to the website of **TORNADO CASH**, accessed via the Wayback Machine's August 5, 2022 archive, the Tornado Cash Trusted Setup Ceremony had a searchable database of participants. OFAC queried this database [redacted] for Tornado Cash founders Storm, Semenov, and Pertsev and identified that each was named in the database, indicating that they were participants in the Trusted Setup Ceremony. [Exhibit 71, pp. 1–3] Based on this information, OFAC assesses that the founders of **TORNADO CASH** contributed to the Trusted Setup Ceremony.

C. (U) ***The Tornado Cash Mixing Service***

(U) According to an August 12, 2022 press release from the Netherlands Fiscal Information and Investigation Service (FIOD), the Financial Advanced Cyber Team (FACT) of the FIOD suspects that **TORNADO CASH** has been used to conceal large-scale criminal money flows, including from (online) thefts of cryptocurrencies (so-called crypto hacks and scams). These included funds stolen through hacks by a group believed to be associated with North Korea. Investigations showed that at least one billion dollars' worth of cryptocurrencies of criminal origin passed through the mixer. [Exhibit 72, p. 1] The sections below describe how **TORNADO CASH**'s mixing service operates, and demonstrate the ways in which **TORNADO CASH** has taken concrete steps to render its services more effective at anonymizing transactions for its users, including through cultivating a large user-base, creating a network of relayers, and engaging in a yearlong anonymity mining program that rewarded users for staking assets in its smart contracts.

1. (U) *The Tornado Cash Mixing Service*: How It Works

(U) **TORNADO CASH** utilizes an array of DAO approved and implemented smart contracts to provide customers with an array of options on multiple blockchains to mix their virtual currencies. The mixing gives customers the ability to obfuscate their transactions — regardless of the source of funds, illicit or otherwise — on the blockchain of their choice. Below demonstrates how **TORNADO CASH** works to accomplish the goal of this obfuscation.

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's August 5, 2022 archive, "Tornado Cash improves transaction privacy by breaking the on-chain link between source and destination addresses. It uses a smart contract that accepts ETH and other tokens deposits from one address and enables their withdrawal from a different address. To maximize privacy, several steps are recommended, such as the use of a relayer for gas payments to withdraw funds from an address with no pre-existing balance." [Exhibit 120, p. 1]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's August 5, 2022 archive, since its inception in 2019, **TORNADO CASH** "has been offering diversified fixed amount pools for six tokens (ETH, DAI,[98] cDAI,[99] USDC,[100] USDT[101] & WBTC [102]) handled by the Ethereum blockchain. Since June 2021, in addition to the Ethereum

---

[98] (U) According to the website of Binance, DAI is on the ERC-20 Network. [Exhibit 92, p. 2]
[99] (U) According to the website of Coinbase, Compound Dai is an algorithmic, autonomous interest protocol created for developers to unlock a range of open finance applications. The Compound is described as a protocol on the Ethereum blockchain that builds asset bundles based on the supply and demand of assets, which are pools of assets with algorithmically derived yield rates. Suppliers (and borrowers) of assets interact directly with the protocol to earn (and pay) variable rates without negotiating maturities, rates, or collateral with peers or counterparties. [Exhibit 93, p. 1]
[100] (U) According to the website of Binance, USDC is USD Coin and is on the ERC-20 Network. [Exhibit 92, p. 2]
[101] (U) According to a May 16, 2022 Forbes article, Tether moves across blockchains like many other digital currencies. There are Tether tokens available on various blockchains, such as the original one with Omni on the Bitcoin platform as well as Liquid, in addition to ETH and TRON (TRX), among others. [Exhibit 124, p. 4]
[102] (U) According to a May 17, 2022 Decrypt article, WBTC stands for Wrapped Bitcoin, simply an ERC-20 token that represents Bitcoin—one WBTC equals one BTC. A BTC can be converted into a WBTC and vice-versa. Being an ERC-20 token makes the transfer of WBTC faster than normal Bitcoin, but the key advantage of WBTC is its integration into the world of Ethereum wallets, DApps, and smart contracts. [Exhibit 125, p. 2]

blockchain, Tornado Cash smart contracts have also been deployed on other side-chains[103] and blockchains. These deployments enabled the tool to either support new tokens or benefit from Layer-2 advantages, such as faster and cheaper transactions. As of today, Tornado Cash is operating on:

- Ethereum Blockchain: ETH (Ethereum), DAI (Dai), cDAI (Compound Dai), USDC (USD Coin),
- USDT (Tether) & WBTC (Wrapped Bitcoin),
- Binance Smart Chain:[104] BNB (Binance Coin),
- Polygon Network:[105] MATIC (Polygon),
- Gnosis Chain (former xDAI Chain): xDAI (xDai),
- Avalanche Mainnet:[106] AVAX (Avalanche),
- Optimism, as a Layer-2 for ETH (Ethereum), and
- Arbitrum One, as a Layer-2 ETH (Ethereum)." [Exhibit 120, p. 2]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's August 5, 2022 archive, "all pools mentioned above can be accessed on tornadocash.eth.link. They operate under the principle of fixed-amount deposits and withdrawals. It means that each token has two to four different pools, allowing transactions of only two to four different fixed amounts (e.g., ETH has four different pools, one for each of these amounts: 0.1, 1, 10 & 100 ETH)." [Exhibit 120, p. 3]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's August 5, 2022 archive, "with the release of Tornado Cash Nova (beta version) in December 2021, an upgraded pool with unique new features has been added to the protocol. Users are no longer constrained by fixed-amount transactions. With the addition of Tornado Cash Nova, they can benefit from the use of an arbitrary amount pool and shielded transfers. Tornado Cash Nova operates on the Gnosis Chain (former xDai Chain) as a Layer2 to optimize speed and cost. It allows deposits and withdrawals of completely customized amounts in ETH. This pool also enables shielded transactions where users can transfer the custody of their token while remaining in the pool." [Exhibit 120, p. 3]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's August 5, 2022 archive, "codes behind Tornado.Cash functioning are fully open-sourced. Working as a DAO, Tornado.Cash governance and mining smart contracts are deployed by its

---

[103] (U) According to a March 7, 2022 CoinDesk article, a sidechain is a separate blockchain network that connects to another blockchain — called a parent blockchain or mainnet — via a two-way peg. [Exhibit 123, p. 3]
[104] (U) According to an April 22, 2021 CoinMarket Cap article, Binance Smart Chain is a new platform that aims to lower transaction costs and provide a space to create DApps and other DeFI. [Exhibit 126, p. 3] According to the "About" page of its website, [redacted] CoinMarket Cap is the world's most-referenced price-tracking website for cryptoassets in the rapidly growing cryptocurrency space. [Exhibit 127, p. 1]
[105] (U) According to a February 22, 2022 Investopedia article, [redacted] Polygon is a cryptocurrency, with a symbol MATIC, and also a technology platform that enables blockchain networks to connection and scale. [Exhibit 129, p. 1]
[106] (U) According to a September 21, 2020 post on Medium, Avalanche is an open-source platform for launching decentralized finance applications and enterprise blockchain deployments in one interoperable, highly scalable ecosystem. [Exhibit 131, p. 4]

community. The protocol also functions with zk-SNARK, which enables zero-knowledge proofs allowing users to demonstrate possession of information without needing to reveal it. The use of this technology is based on open-source research made by Zcash team with the help of the Ethereum community. To set up zk-SNARK initial keys, Tornado.Cash was launched in May 2020 & accounts for 1,114 contributions. This significant number of contributors makes it impossible to compromise the protocol by faking zero-knowledge proofs." [Exhibit 120, p. 4]

(U) According to the website of **TORNADO CASH**, its UI is "hosted on IPFS (InterPlanetary File System) by the community, minimizing risks of data deletion. Indeed, the interface will work as long as at least one user is hosting it." [Exhibit 120, p. 4]

(U) According to the website of **TORNADO CASH**, "behind the Tornado.cash front-end sits a number of Circom circuits, which enable the fundamental privacy guarantees that Tornado.cash users enjoy. These circuits implement the Zero Knowledge protocol that Tornado.cash's smart contracts interface with to prove claims about a user's deposit, such as that it is valid, that is has not already been withdrawn, and in the context of Anonymity Mining, the number of blocks that exist between a note's deposit transaction and its withdrawal. Tornado.cash is best understood as having two separate major components. The core deposit circuit is what most users interact with, proving that a user has created a commitment representing the deposit of some corresponding asset denomination, that they have not yet withdrawn that asset, and that they know the secret that they supplied when generating the initial commitment. The anonymity mining circuits form the basis for the Anonymity Mining program, which incentivizes users to leave their deposits in the contract for longer periods of time, so as to ensure that the Tornado.cash deposit pools maintain a large number of active deposits (thus increasing k-anonymity[107] for other users)." [Exhibit 132, pp. 1, 3–4]

2. (U) *The Tornado Cash Mixing Service*: How the Tornado Cash Smart Contracts Enable Mixing

(U) As will be described below, smart contracts, including those deployed by **TORNADO CASH**, are programs running on the Ethereum blockchain. However, as noted by Coin Center, the smart contracts simply execute "deposit" and "withdrawal" operations. In and of themselves, these operations do not create a mixing service that effectively anonymizes transactions; **TORNADO CASH** also relies on a critical mass of users concurrently depositing and withdrawing transactions to obfuscate links between deposit and withdrawal addresses. As described by **TORNADO CASH** in its January 3, 2020 Medium post, user anonymity depends on the total amount of deposits made to a given smart contract as well as the behavior of other users.

---

[107] (U) According to an April 14, 2021 article by Immuta, the concept of k-anonymity was introduced into information security and privacy back in 1998. It's built on the idea that by combining sets of data with similar attributes, identifying information about any one of the individuals contributing to that data can be obscured. k-Anonymization is often referred to as the power of "hiding in the crowd." Individuals' data is pooled in a larger group, meaning information in the group could correspond to any single member, thus masking the identity of the individual or individuals in question. [Exhibit 197, p. 2]

(U) According to the August 25, 2022, post on the website of Coin Center, "Tornado Cash pools are smart contracts that enable users to transact privately on Ethereum. When prompted by a user, pools will automatically[108] carry out one of two supported operations: "deposit" or "withdraw." Together, these operations allow a user to deposit tokens from one address and later withdraw those same tokens[109] to a different address. Crucially, even though these deposit and withdrawal events occur publicly on Ethereum's transparent ledger, any public link between the deposit and withdrawal addresses is severed. The user can withdraw and use their funds without fear of exposing their entire financial history to third parties. A key principle of Tornado Cash pools is that a user's privacy is derived in large part from the simultaneous usage of the pool by many other users. If the pool had only a single user, it wouldn't matter that the link between the user's deposit and withdrawal addresses was severed: simple inference would make it obvious where the withdrawn tokens came from. Instead, pools are used by many users simultaneously. Think of it like a bank's safe deposit box room. Anyone can go and store valuables in a locked box in that room, and, assuming the locks are good, only the person with the key can ever get those valuables back. Security aside, however, this may or may not be privacy enhancing. If only one person is ever seen going into and out of the room, then we know any valuables in that room are theirs. If, on the other hand, many people frequently go into and out of the room, then we have no way of knowing who controls which valuables in which boxes."
[Exhibit 62, pp. 6–7]

(U) According to a January 3, 2020 Medium post by "Tornado Cash," "although external observers cannot prove which withdrawal comes from which deposit, they can make an educated guess about it. For example:

- If a deposit and a withdrawal are right next to each other, it is very likely that they belong to the same person. We recommend waiting until at least a few deposits are made after yours before withdrawing the note.
- If there is a batch of deposits from one address, and then a batch of the same size of withdrawals to a single address, they are very likely connected. If you need to make multiple withdrawals, try to spread them out and withdraw to addresses not linked with each other.
- Wait until some time has passed after your deposit. Even if there are multiple deposits after yours, they all might be made by the same person that is trying to spam deposits and make users falsely believe that there is large anonymity set when in fact it is lower (also known as a Sybil attack). We recommend waiting at least 24 hours to make sure that

---

[108] (U//~~FOUO~~) Although Coin Center describes this process as "automatic," OFAC assesses that this description is a simplification: as with other transactions on the Ethereum blockchain, the user must broadcast a request for the transaction to be executed on the Ethereum Virtual Machine, and a validator must select the transaction, execute it, and propagate the resulting state change to the rest of the network. This process is described in greater detail in *Section IV.A.2* (***Virtual Currencies*: Ethereum**) above.

[109] (U//~~FOUO~~) OFAC assesses that Coin Center describes users as withdrawing the "same tokens" based on the fact that **TORNADO CASH** provides a non-custodial mixing service. However, this is incorrect in a crucial respect. As detailed in Exhibit 189, tokens on the Ethereum blockchain are represented as account balances assigned to addresses. Consequently, any deposit to a smart contract deployed by **TORNADO CASH** on the Ethereum blockchain is effected by simply updating the aggregate balance of funds associated with that smart contract. Although the user retains custody of their funds in the sense that they alone have the authority to withdraw or transfer the value they deposited, their funds are commingled with assets deposited by other users of the mixing service provided by **TORNADO CASH**."

there were deposits made by multiple people during that time. Check the instance statistics when using it.

- It may also be possible that making deposits or withdrawals only during waking hours of the time zone you are in can reduce your anonymity. A simple way to avoid this problem is to try your best to spread out your deposits and withdrawals as evenly across the 24 hours of each day.
- The anonymity set reflected in Tornado Cash statistics is a total amount of deposits made to a given instance. In practice, it can be lower due to various off-chain factors that are hard to formalize. For example, someone might make a Twitter post about their private transaction — it effectively means that it can be excluded from the anonymity set. Similarly in all other cases when a user deanonymizes himself, his deposit is not contributing any real anonymity. As such, it is in your interest, as well as the interest of all Tornado Cash users, to not publicize the amount that you deposit or the dates and times at which you do so (especially for withdrawals).
- In general, try to avoid any correlations that may suggest that your deposits and withdrawals are linked. A good rule of thumb is to mingle with the crowd." [Exhibit 60, p. 2]

(U) According to an August 10, 2022 CoinDesk article, "Tornado Cash was important not just because it worked (in theory) but because it was trusted, keys burned," Gabagool[110] told CoinDesk. Gabagool is referring to the destruction of the cryptographic keys needed to kick-start privacy-protecting applications, including messaging tools like PGP or blockchains like Monero. This procedure, sometimes called "key shredding," ensures that no one has access to the cryptographic keys needed to decrypt anonymized messages or transactions. Because it typically happens at the early stages of a project, sometimes before there are any users, you often simply have to have faith that this was done and that there are no "backdoors" for bypassing the encryption. Thus, just because an alternate Tornado Cash may be running the same code does not mean you can trust it. This would be all the more complicated considering there will likely be many Tornado Cashes that spring up, causing some market confusion. Further, because Tornado Cash is operated by tumbling transactions, the liquidity of the program had a direct bearing on whether it could successfully scramble[111] the blockchain. If there were multiple Tornado Cashes, and no one could agree which was the "safe" one to use, they would all be less effective. Or in Gabagool's words, it is likely people will redeploy the code, "but it's not a true solve." [Exhibit 57, pp. 4–5]

---

[110] (U) According to an August 15, 2022 article on the website of The Crypto Times, Twitter handle Gabagool.eth's owner is a coder by profession who has also earned online popularity as an on-chain investigator exposing scams and frauds. On August 4, 2022, the trading and liquidity platform Velodrome Finance recovered $350,000 stolen in a hack from a team member. The team member was identified using the alias Gabagool. Gabagool affirmed the act and owned up to it. He revealed that Velodrome had committed the mistake of giving its private key to five team members, including him. After losing money during the crypto bear market, Gabagool withdrew $350,000 in various cryptos which he converted to Ether and sent to Tornado Cash to recover his personal loss. [Exhibit 56, p. 2]

[111] (U) This exhibit is discussing Tornado Cash's tumbling (also known as mixing) services, OFAC assesses that to "Scramble the blockchain" means the process of obfuscating transactions between users of mixing services to make it difficult to trace funds from sender to receiver.

(U//~~FOUO~~) Based on the information presented in Exhibits 57, 60, and 62, OFAC assesses that **TORNADO CASH** provides mixing services to its users not only by facilitating transactions through its smart contracts, but also by cultivating a broad user base that facilitates the anonymity of Tornado Cash transactions. Therefore, OFAC assesses that that **TORNADO CASH** provided mixing services to LAZARUS GROUP* by providing effective mixing services that allowed LAZARUS GROUP* to obfuscate its transactions. *Section V* (**BASES FOR DETERMINATIONS**) below further describes this activity by LAZARUS GROUP*.

3. (U) ***The Tornado Cash Mixing Service*: Anonymity Mining**

(U) As described in detail below, "anonymity mining" was a year-long promotion by **TORNADO CASH** which rewarded users with TORN tokens based on the amount of time they left their deposits in the **TORNADO CASH** smart contract pools.

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's August 5, 2022 archive, until December 2021, the protocol included an anonymity mining system for some of these tokens, allowing its users to earn a governance token (TORN). Users were able to ultimately earn TORN on the Blockchain network by depositing in the ETH, DAI, cDAI & WBTC pools. [Exhibit 120, p. 3]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's June 17, 2022 archive, "anonymity mining is an incentive to increase the level of privacy in any coin-joining or coin-mixing protocols by rewarding participants anonymity points (AP) dependent on how long they hedge their assets in a pool. The Tornado Cash anonymity mining program began on December 18, 2020 and ended on December 18, 2021. Individuals deposited to any one of the anonymity pools that were supported (ETH, WBTC, DAI or cDAI) and were rewarded a fixed amount of AP per block, over the period their deposit remained in the pool. These points could then be exchanged for TORN once claimed. One of the community members created the resource of a mining spreadsheet that helped calculate APYs for each pool and each denomination set within, through estimating the fees required to claim a reward. The Tornado Cash website highly recommended to view this resource and plan one's course of action before expecting to earn yield, and recommended that users always plan when deciding to mine any of the anonymity sets, to be aware that the AP/TORN rate is dependent on supply and demand, therefore, the more people that claim [AP/TORN] the higher the rate becomes, and the less people that claim the lower it becomes." [Exhibit 138, pp. 1, 7]

4. (U) ***The Tornado Cash Mixing Service*: The Relayer Network**

(U//~~FOUO~~) As described in detail below, a network of relayers provides a supplemental anonymizing service for Tornado Cash users withdrawing funds from Tornado Cash pools. In essence, users can pay a third-party (a "relayer") to withdraw funds from the pool on their behalf. **TORNADO CASH** provides this service by maintaining a registry of available relayers, which is deployed to a smart contract. The relayer network also enables the collection of fees from Tornado Cash users, who pay a portion of their withdrawal transaction to the relayer. In turn, the relayers must pay **TORNADO CASH** in TORN to be listed in the relayer registry. As with the other components of **TORNADO CASH**, relayers rely on the coordination, governance, and

structure of the broader **TORNADO CASH** entity for their ability to function as relayers. Therefore, while an individual relayer is arguably an independent operator, OFAC assesses that the ability of Tornado Cash users to execute relayer-facilitated transactions is a functionality provided by the **TORNADO CASH** entity.

(U//~~FOUO~~) According to data from Dune,[112] out of a total of 145,448 withdrawal transactions from **TORNADO CASH**, 121,702[113] used relayers and 23,746 were withdrawn to wallets. [Exhibit 8, p. 1]

a. (U) *The Relayer Network: How Relayers Work*

(U) According to an August 25, 2022 Coin Center article, "relayers" are independent operators that provide an optional service for Tornado Cash users. By default, when users prompt the Tornado Cash pool contracts for withdrawal, the withdrawal account needs to already have Ether to pay the Ethereum network to process the smart contract's operations. However, sending Ether to the withdrawal account prior to withdrawal might create a link between the user's deposit and withdrawal accounts. Relayers allow users to process withdrawals without needing to pre-fund their withdrawal accounts, which helps users maintain privacy when withdrawing. Users select a relayer from a public Relayer Registry. The user then uses their withdrawal account to sign a transaction authorizing the relayer-assisted withdrawal. The user sends this transaction to their selected relayer, who processes the withdrawal on their behalf, earning a fee in the process. According to the Coin Center article, even though they process withdrawals on behalf of users, relayers "never have custody[114] over users' tokens; the smart contract ensures that withdrawn tokens are only ever sent to the user's withdrawal account." [Exhibit 62, pp 15–16]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's June 9, 2022 archive, "relayers form an essential and necessary part of the Tornado Cash ecosystem. Their use guarantees privacy as they solve the infamous "fee payment dilemma": how to pay fees for token withdrawals from a pool while maintaining anonymity? Therefore, relayers act as third parties and manage the entire withdrawal. They pay for transaction fees by deducting them directly from the transferred amount. They also charge an additional fee for their services." [Exhibit 139, p. 1]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's June 9, 2022 archive, "a relayer is chosen by the user interface using the following formula:

- The list of all registered relayers is retrieved from the Relayer Registry smart contract.

---

[112] (U) According to its website, "Dune is a powerful tool for blockchain research. Dune gives you all the tools to query, extract, and visualize vast amounts of data from the blockchain. Dune is unlocking the power of public blockchain data by making it accessible to everyone." [Exhibit 79, p. 1]

[113] (U//~~FOUO~~) This figure represents 83.67 percent of the total withdrawal transactions.

[114] (U) In this context, "custody" has a technical meaning with respect to cryptocurrency. According to the website of CoinDesk, cryptocurrency is essentially a bearer asset, as the person who holds the private keys to a wallet effectively controls (owns) the coins inside. Custodial wallets are wallet services offered by a centralized business such as a cryptocurrency exchange. When a user outsources wallet custody to a business, they are essentially outsourcing their private keys to that institution. Non-custodial wallets do not require the outsourcing of trust to an institution, so no institution can refuse to complete transactions. [Exhibit 97, pp. 2–3]

- For each relayer, calculate a score based on its staked TORN and its fee. The higher the stake, the higher the score is; the higher the fee, the lower the score is. For Ethereum mainnet, the formula used to calculate the score is stake * [1 - 25*(fee-0.33)^2]; for sidechains, the formula is stake * [1 - 11.89*(fee-0.01)^2].
- Then randomly pick a relayer, weighted by its calculated score." [Exhibit 139, pp. 1–2]

(U) The website of **TORNADO CASH**, accessed through the Wayback Machine's June 9, 2022 archive, provides instructions to "anyone [wishing to] become a relayer for the protocol in 6 simple steps through a Relayer Registry User Interface.

1. Warning: Understand & Accept Potential Risks. Before you commit to sharing part of your journey with Tornado Cash users as a relayer, you need to understand & accept all potential risks of being a relayer for the protocol.
2. The first concrete step is to run the Tornado Cash Relayer software for Ethereum Mainnet on your computer. All steps are outlined in the protocol's github. To complete this task successfully, you will have to carefully follow these instructions. Once completed, you will need to insert your url in the input box. It is strongly recommended that you use your own RPC nodes.[115]
3. Set up Ethereum Name Service (ENS)[116] Subdomain. The next steps entail: creating an ENS domain for your relayer; setting up its mainnet subdomain; adding a TXT record with the Relayer URL to the mainnet subdomain. You also have the option to add subdomains with their corresponding TXT records to support chains other than Ethereum. Sidechains relayers use a different version of the Relayer software. Tornado Cash Nova uses its own version of the software.
4. Workers are the addresses that will allow your relayer to send ZK-proofs to users. By default, the first worker is the ENS domain owner's address.
5. With the implementation of a decentralized relayer registry, a staking condition has been introduced as a requirement to become listed on Tornado Cash UI. Keep in mind staking TORN is now necessary to be added to the recommended list of relayers. The minimum staked amount is currently set by Tornado Cash governance at 300 TORN. This threshold can be changed by Tornado Cash governance at any time. When a relayer is used in the Tornado Cash pool, a small amount of TORN is automatically collected from this staked balance by the Staking Reward contract. This element is essential to keep in mind as relayers will need to keep enough TORN locked (~40 TORN in April 2022) to be able to pay back the transaction fee to the staking contract. The collected fees are subsequently distributed among DAO members with locked TORN tokens. TORN are usually locked to participate in on-chain governance (submitting & voting on proposals). Your staked TORN amount is not claimable, and it is non-refundable.
6. Summary: Final Verification & Registration." [Exhibit 139, pp. 1–6]

---

[115] (U) According to the website of Coinbase, a Remote Procedure Call or RPC node is a type of computer server that allows users to read data on the blockchain and send transactions to different networks. [Exhibit 140, p. 1]
[116] (U) According to a May 12, 2022 BeinCrypto Article, ENS refers to Ethereum Name Service, and is a naming protocol that allows humans to use easy-to-remember domain names for their cryptocurrency addresses. The protocol then translates it to a machine-readable address. This process has many similarities to the DNS system we use for the internet. Furthermore, it empowers users with a tool that can unify their online presence and help them step into the realm of web3. [Exhibit 184, p. 1]

(U) According to **TORNADO CASH**'s website, accessed through the Wayback Machine's February 18, 2022 archive, "relayers are used to withdraw to an account with no ETH balance. The relayer sends a withdrawal transaction and takes a part of the deposit as compensation (though the protocol itself does not collect any fees). The relayer cannot change any withdrawal data including recipient address. The Tornado Cash initial developers do not control or play any role in relaying transactions; the relay network is independent and run by the community." [Exhibit 64, p. 7]

(U//~~FOUO~~) Although relayers independently set their fees, and the relayer fees are paid directly to the relayers, **TORNADO CASH** separately collects a per-transaction fee in TORN from relayers. This mechanism is explained in further detail in the remainder of this section and in the next section.

(U//~~FOUO~~) According to an August 25, 2022 Coin Center article, the relayer registry is the smart contract 0x58E8dCC13BE9780fC42E8723D8EaD4CF46943dF2 ("0x58E8d"). According to Coin Center, the relayer registry can be updated pending a Tornado Cash community vote. [Exhibit 62, p. 24] Because the smart contract can be updated by the Tornado Cash community,[117] OFAC assesses that **TORNADO CASH** has the ability to thereby manage the relayer registry.

(U//~~FOUO~~) According to Etherscan, smart contract 0x58E8d has a total of 722 transactions. The most recent transaction to smart contract 0x58E8d occurred on September 20, 2022 and executed the function "stake to relayer." [Exhibit 96, p. 1] Based on the substantial number of transactions, OFAC assesses that Tornado Cash relayers regularly stake to the relayer smart contract or otherwise interact with the relayer smart contract.

(U) According to the website of **TORNADO CASH**, which was archived by the Internet Archive on June 9, 2022, following the execution of Tornado Cash tenth governance proposal, anyone can become a relayer for Tornado Cash users. The only condition to be included on the Tornado Cash UI is to lock a min[imum] of 300 TORN.[118] To remain listed, it is needed to keep enough TORN locked (~ 40 TORN in April 2022) to be able to pay back the transaction fee to the staking contract. Since the implementation of the Relayer Registry proposal, the protocol collects a fee directly from the relayer's staked balance through the "Staking Reward" contract for each withdrawal. This fee percentage may vary from one pool to another and is also subject to change through on-chain governance. Currently[119] it is fixed at 0.3 percent. Some pools remain without fees, either because the instance is too small to assign a fee (0.1 ETH, 100

---

[117] (U) OFAC assesses the term "community" as used in this and other exhibits includes, but is not limited to, holders of TORN and developers of Tornado Cash.
[118] (U) According to a note in the exhibit, this minimum stake can be changed by a governance vote at any time. [Exhibit 139, p. 1]
[119] (U//~~FOUO~~) OFAC assesses that this information was current as of the date it was archived, June 9, 2022.

DAI/USDT, 1000 DAI/USDT), or because there is not enough liquidity on Uni[swap] v3[120] (all cDAI instances). [Exhibit 139, p. 1]

D. (U) *TORNADO CASH's Property and Interests in Property*[121, 122]

1. (U) TORNADO CASH's Interest in the TORNADO CASH Smart Contracts

(U//~~FOUO~~) According to the website of Ethereum, creating a smart contract has a cost because you are using network storage. [Exhibit 58, p. 2] Because creating a contract on the Ethereum blockchain has a cost, OFAC assesses that any given contract has a nonzero monetary value. Because creating a smart contract requires initiating a transaction and paying a fee, OFAC assesses that users create smart contracts because they regard the functionality of the smart contract as having value. Accordingly, OFAC assesses that **TORNADO CASH** regarded smart contracts created on its behalf as having value; that **TORNADO CASH** has derived value from smart contracts created on its behalf; and that therefore **TORNADO CASH** has an interest in such smart contracts.

(U//~~FOUO~~) Based on information presented in this memorandum, OFAC assesses that **TORNADO CASH** has an interest in the smart contracts created on its behalf because use, popularity, and success of the smart contracts increases the economic value of **TORNADO CASH** and of the TORN tokens, including those held by **TORNADO CASH** itself as well as those issued by the DAO to individual DAO members. The DAO issued TORN tokens to early

---

[120] (U//~~FOUO~~) According to Uniswap's website, Uniswap v1 was launched in November 2018 as a proof of concept for automated market makers (AMMs), a type of exchange where anyone can pool assets into shared market making strategies. In May 2020, Uniswap v2 introduced new features and optimizations. As of March 23, 2021, Uniswap v3 was introduced. [Exhibit 141, p. 1] OFAC assesses v3 refers to version three of Uniswap.

[121] (U) The relevant OFAC regulations define "interest," when used with respect to property (e.g., "an interest in property"), as "an interest of any nature whatsoever, direct or indirect." 31 C.F.R. §§ 510.313, 578.309. "Property" and "property interest" are defined as follows:

> The terms *property* and *property interest* include money, checks, drafts, bullion, bank deposits, savings accounts, debts, indebtedness, obligations, notes, guarantees, debentures, stocks, bonds, coupons, any other financial instruments, bankers acceptances, mortgages, pledges, liens or other rights in the nature of security, warehouse receipts, bills of lading, trust receipts, bills of sale, any other evidences of title, ownership, or indebtedness, letters of credit and any documents relating to any rights or obligations thereunder, powers of attorney, goods, wares, merchandise, chattels, stocks on hand, ships, goods on ships, real estate mortgages, deeds of trust, vendors' sales agreements, land contracts, leaseholds, ground rents, real estate and any other interest therein, options, negotiable instruments, trade acceptances, royalties, book accounts, accounts payable, judgments, patents, trademarks or copyrights, insurance policies, safe deposit boxes and their contents, annuities, pooling agreements, services of any nature whatsoever, contracts of any nature whatsoever, and any other property, real, personal, or mixed, tangible or intangible, or interest or interests therein, present, future, or contingent.

31 C.F.R. §§ 510.323, 578.314.

[122] (U) Similar to the physical address of a real estate property that is owned by a blocked person, the digital currency addresses of Tornado Cash smart contracts may refer to interests in property of **TORNADO CASH** and also serve as identifiers associated with **TORNADO CASH**.

backers and users, including the original developers, who can profit by selling tokens on virtual currency exchanges, and changes in the price of TORN tokens appear to correlate with expectations surrounding the success of the smart contracts. TORN owners and the DAO are in this way similar to stockholders, who have an interest in the enterprise, and may benefit from the success of **TORNADO CASH**. Accordingly, the more users that submit virtual currency to the smart contracts to be mixed, the larger the pool becomes, and the more effectively the virtual currency may be mixed, thereby increasing the value of **TORNADO CASH** and of TORN tokens.

(U//~~FOUO~~) According to a May 1, 2020 blog post on the website of Medium, authored by "Tornado Cash," "Tornado Cash is happy to announce that the Tornado Cash Trusted Setup Ceremony has been launched, we ask crypto community to help make Tornado Cash fully trustless by contributing to the ceremony. We plan to end the ceremony on May 10, 2020. If there is high demand, we will keep it open for a couple more days. Tornado Cash utilizes zk-SNARK technology to provide anonymity for withdrawals. The zk-SNARK requires a trusted setup which is a special procedure that generates the prover and verifier keys. In order to make sure that it is done in a secure way, no one is able to fake proofs or steal user funds it should be done in a decentralized way. To fake zk proofs, an attacker must compromise every single participant of the ceremony. Therefore, the probability of it goes down as the number of participants goes up. The purpose of the ceremony is to generate Verifier smart contract. After completion, our team will update all Verifiers in all instances and set the operator address to zero. At this point Tornado Cash smart contracts will become completely immutable and unstoppable." [Exhibit 39, pp. 1–3] Because organizing and coordinating these setup ceremonies would require the expenditure of time and effort, OFAC assesses that a smart contract that has undergone this setup ceremony is more valuable than one that has not. Based on **TORNADO CASH** announcing the setup ceremony and soliciting participants in it, OFAC assesses that value created through this setup ceremony was generated for the benefit of **TORNADO CASH**.

(U//~~FOUO~~) According to a December 15, 2021 post on the website of Medium, authored by "Tornado Cash," **TORNADO CASH** introduced "Tornado Cash Nova," an upgraded Tornado Cash pool[123] presenting unique features focused on improving user experience and expanding the protocol functionalities. This pool will allow users to deposit and withdraw arbitrary amounts of ETH. Up to now, all Tornado Cash pools had one thing in common: users could only deposit and withdraw a fixed amount of a given token within each pool. With the arrival of the Nova pool, this statement will no longer be true. An improved v3 of the Tornado Cash protocol is being currently prepared. This incoming version mainly focuses on enhancing users' experience. Some handy new features are planned to bring more flexibility and possibilities to the use of the protocol. With its customized amounts and shielded transfers, "Tornado Cash Nova" is the first step towards this new and improved version of Tornado Cash. Future plans for the protocol include the possibility of making atomic swaps[124] within a shielded pool, as well as a pool that

---

[123] (U//~~FOUO~~) Given that the "pools" described in this exhibit receive funds and facilitate obfuscation, OFAC assesses that the referenced "pools" are references to Tornado Cash smart contracts.

[124] (U) According to an August 14, 2022 Investopedia article, "Atomic Swap Definition," an atomic swap is an exchange of cryptocurrencies from separate blockchains. The swap is conducted between two entities without a

will be able to support ERC-20 tokens & NFT. [Exhibit 15, pp. 2, 5] OFAC assesses that these efforts by **TORNADO CASH** to advertise improvements in its mixing service in aid of maximizing its number of users, as evidenced in Exhibit 15 and throughout this memorandum, show that **TORNADO CASH** has an interest in the deployed smart contracts, including those that contain these touted improvements.

2. (U) TORNADO CASH's Interest in the TORN Smart Contract

(U//~~FOUO~~) As described above in *Sections IV.B.2* (***TORNADO CASH*: Decentralized Autonomous Organization (DAO)**) and *IV.C.6* (***The Tornado Cash Mixing Service*: The Relayer Network**), **TORNADO CASH** created the TORN token through a smart contract deployed on the Ethereum blockchain. OFAC assesses that **TORNADO CASH** thus controlled governance and disbursement of TORN tokens. **TORNADO CASH** structured payouts of TORN tokens so that they incentivize use of the Tornado Cash mixing service. In particular, **TORNADO CASH** airdropped TORN to users of the service. In addition, the "anonymity mining" program rewarded users with TORN based on the length of time that they held assets in Tornado Cash smart contract pools. As described above, the greater the quantity of assets held in the Tornado Cash smart contract pools, the greater the efficacy of the Tornado Cash mixing service. Therefore, by implementing the anonymity mining program, **TORNADO CASH** used its control over disbursement of TORN tokens to enhance the efficacy of the Tornado Cash mixing service, increasing the value of its service and smart contracts.

(U//~~FOUO~~) As described above, **TORNADO CASH** disbursed only a portion of the maximum total supply of 10 million TORN tokens. **TORNADO CASH** distributed a majority of TORN tokens to the custody of **TORNADO CASH** itself through several smart contracts.

(U) According to Etherscan, as of October 1, 2022, eight of the top ten addresses holding the most TORN tokens are Tornado Cash smart contract addresses. The address that holds the most TORN tokens is the Tornado Cash Governance Vesting smart contract, which holds 4,125,000 TORN tokens worth approximately $26.3 million. The address that holds the third-most TORN tokens is the Tornado Cash Governance smart contract, which holds approximately 1,258 TORN tokens worth approximately $8 million. [Exhibit 90, p. 1]

(U//~~FOUO~~) As described in *Section IV.B.2* (***TORNADO CASH*: Decentralized Autonomous Organization (DAO)**), **TORNADO CASH** has used the TORN it controlled to fund development and enhancement of the **TORNADO CASH** mixing service. It has offered to pay TORN to contributors to **TORNADO CASH** and offered bug bounties in TORN to those who identified security vulnerabilities in its smart contracts.

(U//~~FOUO~~) Based on the explanation in Exhibit 5, showing that relayers must pay a fee directly to the **TORNADO CASH** DAO, and based on the fact that TORN holders can receive a portion of these fees based on the amount of TORN they have staked, OFAC assesses that **TORNADO**

---

third party's involvement. The idea is to remove centralized intermediaries like regulated exchanges and give token owners total control. [Exhibit 68, p. 1]

CASH has an interest in user transactions that are withdrawn through relayers, and in the TORN tokens used in that process.

3. (U) **TORNADO CASH's Interest in Pool and Relayer Smart Contracts**

(U//~~FOUO~~) According to the August 25, 2022 post on the website of Coin Center, "a key principle of Tornado Cash pools is that a user's privacy is derived in large part from the simultaneous usage of the pool by many other users. If the pool had only a single user, it would not matter that the link between the user's deposit and withdrawal addresses was severed: simple inference would make it obvious where the withdrawn tokens came from. Instead, pools are used by many users simultaneously. Think of it like a bank's safe deposit box room. Anyone can go and store valuables in a locked box in that room, and, assuming the locks are good, only the person with the key can ever get those valuables back. Security aside, however, this may or may not be privacy enhancing. If only one person is ever seen going into and out of the room, then we know any valuables in that room are theirs. If, on the other hand, many people frequently go into and out of the room, then we have no way of knowing who controls which valuables in which boxes." [Exhibit 62, pp. 6–7] Because the efficacy of **TORNADO CASH** as a mixer depends on a critical mass of users depositing funds to its pool smart contracts, OFAC assesses that **TORNADO CASH**'s efforts to entice more and more users to deposit funds into its smart contracts is evidence of **TORNADO CASH**'s interest in in the funds that users have deposited into its smart contracts.

(U//~~FOUO~~) According to data from Dune, out of a total of 145,448 withdrawal transactions from Tornado Cash, 121,702 used relayers and 23,746 were withdrawn to wallets. [Exhibit 8, p. 1] Because relayers were used in the substantial majority of withdrawal transactions from **TORNADO CASH**, OFAC assesses that tokens held in the **TORNADO CASH** smart contract pools have the potential to generate fees for **TORNADO CASH** because of the fees required to use relayers. OFAC therefore assesses that **TORNADO CASH** has an interest in such funds.

(U//~~FOUO~~) According to data from Dune, in the week of August 29, 2022, relayer fees for Tornado Cash paid to Governance in U.S. dollars were $76,135. [Exhibit 77, p. 1] Based on this information, OFAC assesses that **TORNADO CASH** was receiving fees generated through use of its pool and relayer smart contracts. These facts further evidence that **TORNADO CASH** has an interest in the pool and relayer smart contracts.

(U//~~FOUO~~) According to the "Staking" section of **TORNADO CASH**'s website, with the introduction of a decentralized relayer register, a staking reward has been implemented for all holders with locked TORN in the governance contract. TORN holders can still lock their tokens into the governance contract as they used to for governance purposes. The significant difference is that they are now able to receive a portion of the fees collected by the protocol from relayers. In a nutshell, for each withdrawal through the relayer method, the chosen relayer has to pay a fee to the protocol from the staked balance (that should still be maintained above the 300 TORN threshold). Currently, this fee has been fixed at 0.3 percent by the governance and can be changed at any time through an on-chain [proposal of change and corresponding vote].

[Exhibit 5, p. 1] Based on the fact that the Tornado Cash Governance Contract[125] receives a fee from each withdrawal through the relayer method, OFAC assesses that **TORNADO CASH** has an interest in such withdrawals.

(U//~~FOUO~~) As described previously in *Section IV.C.6* (***The Tornado Cash Mixing Service*: The Relayer Network**), becoming a relayer listed on the **TORNADO CASH** UI requires staking TORN to the Tornado Cash Governance Contract. **TORNADO CASH** collects a fee from this staked TORN each time the relayer is used to facilitate a withdrawal from the **TORNADO CASH** pool smart contracts. In return, the relayer receives a portion of the withdrawal (for example, a relayer receives ETH for withdrawals from ETH pools). As **TORNADO CASH** deducts fees from the relayer's staked TORN, the relayer must acquire and stake more TORN in order to continue acting as a relayer. Consequently, higher volume usage of the Tornado Cash mixing service, resulting in greater numbers of withdrawals via relayers, creates additional demand for TORN tokens. Therefore, based on **TORNADO CASH**'s interest in and holdings of TORN tokens, OFAC assesses that **TORNADO CASH** has an interest in its mixing service as deployed via the pool, relayer, and other smart contracts.

E. (U) *Foreign Person Property Interest Nexus*[126]

1. (U) Interest of North Korea

(U) According to a February 9, 2021 Reuters[127] article, a preliminary United Nations (UN) inquiry into the theft of $281 million worth of assets from a cryptocurrency exchange in September 2020 "strongly suggests" links to North Korea—with industry analysts pointing to Seychelles-based KuCoin as the victim of one of the largest reported digital currency heists. A confidential report by independent sanctions monitors to UN Security Council members said blockchain transactions related to the hack also appeared to be tied to a second hack last October when $23 million was stolen. "Preliminary analysis, based on the attack vectors and subsequent efforts to launder the illicit proceeds, strongly suggests links to the DPRK," the monitors wrote. They accuse Pyongyang of using stolen funds to support its nuclear and ballistic missile

---

[125] (U) As detailed above, the Tornado Cash governance contract plays an essential role in the operation and governance of **TORNADO CASH** and of the service provided by **TORNADO CASH**.

[126] (U) Section 203 of the International Emergency Economic Powers Act ("IEEPA"), authorizes the President to:

> investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit, any acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, *any property in which any foreign country or a national thereof has any interest* by any person, or with respect to any property, subject to the jurisdiction of the United States.

50 U.S.C. § 1702(a)(1)(B) (emphasis added). Thus, OFAC may block or prohibit even domestic transactions where a foreign country or national thereof has an interest in the underlying property.

[127] (U) According to the homepage of its website, accessed on April 29, 2022, Reuters, the news and media division of Thomson Reuters, is the world largest multimedia news provider, reaching billions of people worldwide every day. Reuters provides business, financial, national, and international news to professionals via desktop terminals, the world's media organizations, industry events, and directly to consumers. [Exhibit 147, p. 16]

programs to circumvent sanctions. While the report did not name the victim of the attack, digital currency exchange KuCoin reported the theft of $281 million in bitcoin and various other tokens on September 25, 2020. [Exhibit 180, pp. 1–2]

(U) According to a February 2022 Chainalysis report, LAZARUS GROUP* first gained notoriety from its Sony Pictures and WannaCry cyberattacks, but it has since concentrated its efforts on cryptocurrency crime—a strategy that has proven immensely profitable. From 2018 on, the group has stolen and laundered massive sums of virtual currencies every year, typically in excess of $200 million. The most successful individual hacks, one on KuCoin and another on an unnamed cryptocurrency exchange, each netted more than $250 million alone. And according to the UN security council, the revenue generated from these hacks goes to support North Korea's WMD and ballistic missile programs. [Exhibit 178, p. 114]

(U//~~FOUO~~) According to blockchain analysis conducted by OFAC, funds stolen in the KuCoin hack were subsequently transferred to Ethereum address 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291, which is attributed by Chainalysis to **TORNADO CASH**. This transfer of funds occurred between October 19, 2020 and October 21, 2020, in a series of 134 transactions of 100 ETH each. The total value of these transfers was over $5 million. [Exhibit 181, p. 2]

(U) According to the website of Etherscan, address 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291 is a Tornado Cash smart contract and was deployed by another Tornado Cash smart contract, address 0x8589427373D6D84E98730D7795D8f6f8731FDA16. [Exhibit 182, p. 1]

(U//~~FOUO~~) Based on the above information, OFAC assesses that threat actors acting on behalf of North Korea transferred funds to **TORNADO CASH** between October 19, 2020 and October 21, 2020. This attribution is strengthened by North Korean threat actors' repeated use of the service provided by **TORNADO CASH** to launder stolen funds, as described further throughout this memorandum.

(U//~~FOUO~~) As described previously in Exhibit 4, **TORNADO CASH** airdropped TORN tokens to addresses that had used its mixing service prior to December 6, 2020. Because North Korean threat actors used the service provided by **TORNADO CASH** during this timeframe, and because **TORNADO CASH** did not implement any mechanism to prevent illicit actors from benefiting from its airdrop, OFAC assesses that North Korean threat actors received TORN in **TORNADO CASH**'s airdrop, and consequently received the ability to participate in voting on changes to the service provided by **TORNADO CASH**.

(U//~~FOUO~~) As described previously in *Section IV.B.2* (***TORNADO CASH*: Decentralized Autonomous Organization (DAO)**), TORN is **TORNADO CASH**'s governance token. In addition, as described in *Section IV.C.6* (***The Tornado Cash Mixing Service*: The Relayer Network**), value generated through use of the Tornado Cash mixing service accrues to holders of TORN through distribution of fees and an increase in the value of TORN. Therefore, North Korea's ownership of TORN tokens created an interest of North Korea in **TORNADO CASH**.

2. (U) **Foreign Person Founders and Developers**

(U) The below individuals have been identified as key developers of **TORNADO CASH** who likely received a portion of the 30% of available TORN tokens that were locked for a period of three years, as described in Exhibit 4:

- (U//~~FOUO~~) According to an August 19, 2022[128] CoinMarket Cap article, "Another Russian national that is in the crosshairs of the Dutch authorities is Alexey Pertsev the arrested Tornado Cash developer. [Exhibit 11, p. 2] OFAC assesses that Alexey Pertsev is a Russian national because Exhibit 11 refers to Alexey Pertsev as "another Russian national."
- (U) According to an August 24, 2022 report by Kharon,[129] Alexey Pertsev, a resident of the Netherlands, is a founder and the CEO of PepperSec, according to personal and company profiles reviewed by Kharon. In 2017, Alexey Pertsev was an information security specialist and developer of smart contracts for DIGITAL SECURITY OOO*,[130] according to an archived version of the company's website reviewed by Kharon. DIGITAL SECURITY OOO* is a Russian entity designated by the U.S. Treasury Department in 2018 for providing material and technological support to the FEDERAL SECURITY SERVICE* (FSB*)[131], Russia's primary security agency. Treasury alleged that, as of 2015, DIGITAL SECURITY OOO* worked on a project that would increase the offensive cyber capabilities of Russia's intelligence services. [Exhibit 42, p. 3]
- (U//~~FOUO~~) According to Crunchbase,[132] Roman Semenov, a co-founder of **TORNADO CASH**, is located in Moscow, Russia, and is a co-founder of the company PepperSec. [Exhibit 13, p. 1] Given the fact that Roman Semenov is located in Russia, OFAC assesses that Roman Semenov is a Russian national.

3. (U) **Foreign Person TORN Token Holders**

(U) According to the website of Etherscan, accessed August 19, 2022, the TORN holdings of the following addresses[133] attributed to foreign entities are as follows:

---

[128] (U//~~FOUO~~) While there is no date on this article, it states that it was updated 5 days ago, and was accessed by OFAC on August 24, 2022. Therefore, OFAC assesses the article was updated on August 19, 2022.
[129] (U) According to its website, Kharon's risk data and software solutions are unparalleled in precision and depth, powering compliance, risk management, investigations, and analytic operations at the world's leading institutions. [Exhibit 43, p. 2]
[130] (U) On June 11, 2018, DIGITAL SECURITY OOO* was designated by the Department of the Treasury pursuant to E.O. 13694 for providing material and technological support to the FSB*. [Exhibit 44, p. 1–2]
[131] (U) On December 28, 2016, the FSB* was listed in the annex of E.O. 13694, as amended. [Exhibit 45, p. 3] On March 2, 2021, the FSB* was designated by the U.S. Department of State pursuant to E.O. 13382 for having engaged, or attempted to engage, in activities or transactions that have materially contributed to, or pose a risk of materially contributing to, the proliferation of weapons of mass destruction or their means of delivery (including missiles capable of delivering such weapons), including any efforts to manufacture, acquire, possess, develop, transport, transfer or use such items, by Russia. [Exhibit 46, p. 4]
[132] (U) According to its website, Crunchbase allows users to search, track, and monitor companies' customers care about using best-in-class private company data. [Exhibit 33, p. 1]
[133] (U) The list below contains the label for the address on the website on the website of Etherscan, rather than the address itself.

- Binance 8[134]: 1,658,151 TORN;
- OKEx: 218,635 TORN;
- Binance 14: 50,174 TORN
- Binance 15: 11,746 TORN
- Binance 16: 13,341 TORN
- 1inch: 6,069 TORN [Exhibit 10, pp. 1–2]

(U) According to an October 29, 2020 Forbes article, Binance is currently known to be Cayman Islands based, but the exchange first launched in Shanghai. Later as the Chinese government cracked down on cryptocurrency trading, the company moved its headquarters to Japan and then Malta. In May 2020 [Binance founder Changpeng Zhao] told former Forbes staffer Laura Shin that Binance's headquarters were wherever he was. His answer wasn't necessarily evasive but presented as a rally cry for blockchain's ideals of decentralized power. [Exhibit 98, p. 7]

(U) According to its website OKEx is a virtual currency exchange located in Seychelles. [Exhibit 31, p. 1]

(U) According to the Securities Exchange Commission, 1inch is registered in the British Virgin Islands. [Exhibit 32 p. 1]

(U) According to the website of Etherscan, as of October 1, 2022, an address attributed to Binance was the second-largest holder of TORN and held over 18 percent of all TORN, equivalent to approximately $11.5 million. [Exhibit 90, p. 1]

(U) According to the website of Binance, as of October 1, 2022, TORN tokens are available for trade and were trading at $6.37. [Exhibit 37, p. 1]

(U) According to the website of Binance, [redacted] Binance claims that it is "unable to provide services to U.S. users. Binance.US (BAM Trading Services) is a U.S.-regulated cryptocurrency trading platform. In approved states, U.S. customers can use Binance.US to buy and sell over 50 cryptocurrencies with low fees." [Exhibit 91, p. 1]

(U) According to the website of Binance.US, [redacted] Binance.US currently support 100+ digital assets. TORN was not included in this list of assets. [Exhibit 92, pp. 1, 4]

(U//~~FOUO~~) Based on the above information, OFAC assesses that user deposits of TORN held in custody by Binance are at least in substantial part the property of non-U.S., foreign persons.

V. (U) BASES FOR DETERMINATIONS

A. (U) *Designation Pursuant to E.O. 13694, as Amended*

[134] (U//~~FOUO~~) OFAC assesses that the numbering of these addresses distinguishes multiple addresses that have been attributed to the same entity.

(U//~~FOUO~~) In March 2022, DPRK's LAZARUS GROUP* carried out a heist of the Axie Sky Mavis Ronin Network, which is the largest cyber heist to date. LAZARUS GROUP* stole over $600 million worth of the virtual currency Ether and subsequently carried out an extensive money laundering operation. The money laundering operation was an effort to separate the source and destination of funds. **TORNADO CASH**, a provider of virtual currency mixing services, received the majority of these funds and provided its obfuscating services to LAZARUS GROUP* to make it more difficult for authorities to trace the funds from the victim to the cyber actors who carried it out.

1. (U) ***Sky Mavis-Ronin Bridge Heist*** (Cyber-Enabled Activity)

   a. (U//~~FOUO~~) *The **Sky Mavis-Ronin Bridge Heist** is a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.*

(U) According to a March 30, 2022 Reuters article, hackers have stolen virtual currency worth almost $615 million from a blockchain project linked to the popular online game Axie Infinity. Ronin, a blockchain network that lets users transfer crypto in and out of the game, said on Tuesday, March 29, 2022, that the theft happened on March 23, 2022, but was not detected until almost a week later. Ronin produces a digital wallet for storing crypto, and a "bridge" that allows users to move funds into and out of the online game. This is where crypto was stolen from. Sky Mavis is a Vietnam-based company that launched Axie Infinity in 2018.[135] [Exhibit 145, pp. 3–4]

(U) According to a March 30, 2022 *Barron's*[136] article, the ***Sky Mavis-Ronin Bridge Heist*** is disconcerting partly because of the size of the theft, but also because of how it transpired. Ronin is managed by just nine computer "nodes" that validate transactions in the network. Typically, it takes a majority of nodes to form a consensus on the validity of a transaction, enabling it to be recorded on the blockchain. In this case, the hackers gaining control of just five nodes did the trick. [Exhibit 146, pp. 1–2]

(U//~~FOUO~~) [redacted]

[135] (U) Due to the association of Sky Mavis and Axie Infinity with this heist, OFAC will refer to it as the ***Sky Mavis-Ronin Bridge Heist***, although some media reports also refer to it as the "Ronin heist."
[136] (U) According to the "About" page of its website, accessed on April 14, 2022, *Barron's* is a financial journal whose founder believed the press should be Wall Street's watchdog. [Exhibit 148, p. 4]

[redacted][137][redacted][138][redacted][139][redacted] [Exhibit 153, p. 10]

(U//~~FOUO~~) [redacted][40][redacted] [Exhibit 153, p. 11]

(U//~~FOUO~~) According to an April 14, 2022 Federal Bureau of Investigation (FBI) press statement, the FBI continues to combat malicious cyber activity including the threat posed by DPRK to the United States and its private sector partners. Through its investigation FBI was able to confirm LAZARUS GROUP* cyber actors associated with DPRK, are responsible for the theft of $620 million ETH reported on March 29, 2022. The FBI in coordination with Treasury and other U.S. government partners, will continue to expose and combat DPRK's use of illicit activities, including cybercrime and virtual currency theft to generate revenue for the regime. [Exhibit 159, p. 1] This press statement is referring to the ***Sky Mavis-Ronin Bridge Heist***, which was reported on March 29, 2022, given the approximate $620 million value and occurrence on March 29, as described in Exhibit 145 and Exhibit 146 and attributed to the DPRK by the FBI in Exhibit 159 [redacted], in addition to OFAC and FBI's close coordination on this matter. Accordingly, OFAC assesses that the ***Sky Mavis-Ronin Bridge Heist*** is a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States.

> b. (U//~~FOUO~~) *The **Sky Mavis-Ronin Bridge Heist** is a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.*

(U//~~FOUO~~) According to the April 14, 2022 FBI press statement, the FBI continues to combat malicious cyber activity including the threat posed by DPRK to the United States and our private

---

[137] (U) According to a July 31, 2020 CoinDesk Article, a spear-phishing attack is a targeted attempt to steal information such as account details or financial information from a particular individual. [Exhibit 150, p. 3]
[138] (U) According to a February 25, 2022 Medium article, validators store a copy of the blockchain and must perform certain functions to keep the system secure. [Exhibit 154, p. 1]
[139] (U) According to an October 14, 2020 Medium article, a third-party validator is a validator-as-a-service that have dedicated infrastructure and personnel to solely run validators for other people. [Exhibit 156, p. 1]
[140] (U) According to a January 6, 2021 CoinDesk article, RAT refers to a Remote Access Tool. [Exhibit 158, p. 3]

sector partners. Through its investigation FBI was able to confirm LAZARUS GROUP* cyber actors associated with DPRK are responsible for the theft of $620 million ETH reported on March 29, 2022. The FBI in coordination with Treasury and other U.S. government partners, will continue to expose and combat DPRK's use of illicit activities, including cybercrime and virtual currency theft to generate revenue for the regime. [Exhibit 159, p. 1] This press statement is referring to the ***Sky Mavis-Ronin Bridge Heist***, which was reported on March 29, 2022, given the approximate $620 million value and occurrence on March 29, as described in Exhibit 145 and Exhibit 146 and attributed to DPRK by the FBI in Exhibit 159 [redacted].

(U) According to an April 14, 2020 DPRK Cyber Threat Advisory jointly authored by the State Department, Treasury Department, Department of Homeland Security, and the FBI, DPRK's malicious cyber activities threaten the United States and the broader international community and, in particular, pose a significant threat to the international financial system. Under pressure of robust U.S. and UN sanctions, DPRK has increasingly relied on illicit activities, including cybercrime, to generate revenue for its WMD and ballistic missile programs. In particular, the United States is deeply concerned about DPRK's malicious cyber activities. DPRK has the capability to conduct disruptive and harmful cyber activity that is wholly inconsistent with the growing international consensus on what constitutes responsible State behavior in cyberspace. [Exhibit 174, p. 1]

(U) According to Annex I in the April 14, 2020 joint cyber threat advisory, the Office of the Director of National Intelligence's Annual Worldwide Threat Assessments of the U.S. Intelligence Community (IC) noted in 2019 that DPRK poses a significant cyber threat to financial institutions, remains a cyber-espionage threat, and retains the ability to conduct disruptive cyber-attacks. DPRK continues to use cyber capabilities to steal more than $1.1 billion from financial institutions across the world—including a successful cyber heist of an estimated $81 million from Bangladesh Bank. [Exhibit 174, p. 9]

(U//~~FOUO~~) Given the facts that DPRK executed the ***Sky Mavis-Ronin Bridge Heist***, as demonstrated in Exhibit 159, and DPRK uses funds derived from malicious cyber activities to fund its WMD and ballistic missiles programs, as described in Exhibit 174, OFAC assesses that the ***Sky Mavis-Ronin Bridge Heist*** is reasonably likely to result in, or has materially contributed to, a significant threat to the national security of the United States.

> c. (U//~~FOUO~~) *The **Sky Mavis-Ronin Bridge Heist** is a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.*

(U//~~FOUO~~) [redacted]

[redacted][141] [redacted] [Exhibit 153, p. 10]

(U) According to a March 29, 2022 Bloomberg article, on March 23, 2022 hackers stole about $600 million from a blockchain network connected to the popular Axie Infinity online game in one of the biggest crypto attacks to date. Computers known as nodes operated by Axie Infinity maker Sky Mavis and the Axie DAO that support a so-called bridge software that lets people convert tokens into ones that can be used on another network were attacked, with the hacker draining what's known as the ***Sky Mavis-Ronin Bridge Heist*** of 173,600 ETH and $25.5 million USDC tokens in two transactions. [Exhibit 171, pp. 1–2]

(U) According to an August 30, 2019 U.N. Report from the Panel of Experts, the panel investigated the widespread and increasingly sophisticated use of cyber means by DPRK to illegally force the transfer of funds from financial institutions and virtual currency exchanges, launder stolen proceeds, and generate income in evasion of financial sanctions. In particular, large-scale attacks against virtual currency exchanges allow DPRK to generate income in ways that are harder to trace and subject to less government oversight and regulations than the traditional banking sector. DPRK cyber actors raise money for their country's WMD program with total proceeds to date estimated at up to $2 billion. [Exhibit 168, p. 4]

(U//~~FOUO~~) OFAC assesses that the ***Sky Mavis-Ronin Bridge Heist*** had the purpose or effect of causing a significant misappropriation of funds for commercial or competitive advantage, namely, the advantage of an injection of an estimated $620 million in difficult-to-trace funds into DPRK's WMD program—funds that would not have been available to DPRK but for the illicit cyber-enabled activity.

2. (U) **TORNADO CASH** (Entity)

(U//~~FOUO~~) ***TORNADO CASH*** *has materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of the* ***Sky Mavis-Ronin Bridge Heist****, an activity described in section 1(a)(ii) of E.O. 13694, as amended.*

(U) According to a March 11, 2022, Finance Brokerage[142] article, "one of the founders of Tornado Cash, one of the most popular obfuscation services for crypto transactions, said it does not have to comply with sanctions imposed after Russia attacked Ukraine. The protocol is designed to preserve privacy by disconnecting the sender and receiver addresses in transactions over the Ethereum blockchain. The project is based on smart contracts which means ready-made

[141] (U) [redacted]

[142] (U) According to the "About Us" page of its website, [redacted] Finance Brokerage is a comprehensive financial and market news platform that is accessed by thousands of people all around the world. [Exhibit 162, p. 2]

software programs rather than individuals making decisions. It also does not offer to host services, nor does it have a central host for its website. Individuals can access Tornado Cash using the Ethereum Name Service. It [Ethereum Name Service] is a credential free distributed naming system that the co-founder says helps make monitoring users impossible." [Exhibit 161, p. 1]

(U) According to an April 4, 2022 Bloomberg article, "a hacker moved some of the roughly $600 million in cryptocurrency stolen from the Axie Infinity play-to-earn gaming platform to a service that helps users mask transactions. About 2,000 ETH tokens, valued at around $7 million, that were lifted from Axie Infinity's Ronin software bridge[143] last month [March 2022] were moved Monday [April 4] to Tornado Cash, blockchain data shows. Tornado Cash is designed to preserve privacy on the Ethereum blockchain. Its technology breaks the link between the sender and receiver's addresses on transactions sent to the Ethereum blockchain. The protocol has been used in the past by hackers who took $34 million from Crypto.com. "Tracking funds after any mixer, including Tornado Cash, is a probabilistic method and we cannot be 100 percent certain," blockchain analysis firm Merkle Science wrote in an email response. The main ETH address used by the hackers who attacked Axie Infinity's Ronin blockchain sent 2,001 ETH to another ETH address earlier Monday [April 4]. The second ETH address then sent 2,000 ETH in batches of 100 ETH each to Tornado Cash, blockchain data shows. The transactions were confirmed by blockchain data firm Nansen." [Exhibit 163, p. 1]

(U//~~FOUO~~)

144

145

[143] (U//~~FOUO~~) OFAC assesses that the theft of roughly $600 million in cryptocurrency from "Axie Infinity's Ronin Software bridge" is referring to the ***Sky Mavis-Ronin Bridge Heist***, given the approximate $620 million value and occurrence on March 29, 2022, as described in Exhibit 145 and Exhibit 146.

[144] (U//~~FOUO~~)

[145] (U)

[redacted] [Exhibit 153, pp. 10–11]

(U//~~FOUO~~) Given that the funds of ***Sky Mavis-Ronin Bridge Heist*** were processed through the service provided by **TORNADO CASH** [redacted], OFAC assesses that **TORNADO CASH** has provided material support to the ***Sky Mavis-Ronin Bridge Heist***, namely, by providing transaction obfuscation services meant to separate the trail of the source of the stolen funds to the cyber-enabled malicious actors.

(U//~~FOUO~~) Additional information to support OFAC's designation of **TORNADO CASH** is available in the classified addendum to this memorandum.

B. (U) ***Designation Pursuant to E.O. 13722***

(U) **TORNADO CASH** (Entity)

(U//~~FOUO~~) ***TORNADO CASH*** *has materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, the Government of North Korea. (E.O. 13722)*

(U) According to a September 13, 2019 U.S. Treasury Department Press release, "Today, OFAC announced sanctions targeting three North Korean state-sponsored malicious cyber groups responsible for North Korea's malicious cyber activity on critical infrastructure. Today's actions identify North Korean hacking groups commonly known within the global cyber security private industry as "Lazarus Group," "Bluenoroff," and "Andariel" as agencies, instrumentalities, or controlled entities of the Government of North Korea pursuant to E.O. 13722, based on their relationship to the RECONNAISSANCE GENERAL BUREAU* (RGB*). LAZARUS GROUP*, Bluenoroff, and Andariel are controlled by the U.S.- and UN-designated RGB*, which is North Korea's primary intelligence bureau." [Exhibit 113, pp. 1–2]

(U) According to a March 30, 2022 Reuters article, hackers have stolen virtual currency worth almost $615 million from a blockchain project linked to the popular online game Axie Infinity. Ronin, a blockchain network that lets users transfer crypto in and out of the game, said on Tuesday, March 29, 2022, that the theft happened on March 23, 2022, but was not detected until almost a week later. Ronin produces a digital wallet for storing crypto, and a "bridge" that allows users to move funds into and out of the online game. This is where crypto was stolen from. Sky Mavis is a Vietnam-based company that launched Axie Infinity in 2018. [Exhibit 145, pp. 3–4]

(U) According to an April 14, 2022 FBI press statement, "The FBI continues to combat malicious cyber activity including the threat posed by DPRK to the United States and our private sector partners. Through our investigation we were able to confirm LAZARUS GROUP* cyber actors associated with DPRK, are responsible for the theft of $620 million ETH reported on March 29, 2022. The FBI in coordination with Treasury and other U.S. government partners, will continue to expose and combat DPRK's use of illicit activities, including cybercrime and virtual currency theft to generate revenue for the regime." [Exhibit 159, p. 1] This press

statement is referring to the same stolen virtual currency crime described in Exhibit 145, which was reported on March 29, 2022, given the approximate $620 million value and occurrence on March 29, as described in Exhibit 145.

(U) According to an April 18, 2022, Department of Homeland Security, Cybersecurity Infrastructure and Security Agency (CISA) advisory, the FBI, and Treasury are issuing this joint Cybersecurity Advisory (CSA) to highlight the cyber threat associated with cryptocurrency thefts and tactics used by a North Korean state-sponsored advanced persistent threat (APT) group since at least 2020. This group is commonly tracked by the cybersecurity industry as LAZARUS GROUP*, APT38, Bluenoroff, and Stardust Chollima. [Exhibit 167, p. 1]

(U) According to an August 30, 2019 U.N. Report from the Panel of Experts, the panel investigated the widespread and increasingly sophisticated use of cyber means by DPRK to illegally force the transfer of funds from financial institutions and virtual currency exchanges, launder stolen proceeds, and generate income in evasion of financial sanctions. In particular, large-scale attacks against virtual currency exchanges allow DPRK to generate income in ways that are harder to trace and subject to less government oversight and regulations than the traditional banking sector. DPRK cyber actors raise money for their country's WMD program with total proceeds to date estimated at up to $2 billion. [Exhibit 168, p. 4]

(U) According to an April 14, 2020 DPRK Cyber Threat Advisory jointly authored by the State Department, Treasury Department, Department of Homeland Security, and the FBI, DPRK's malicious cyber activities threaten the United States and the broader international community and, in particular, pose a significant threat to the international financial system. Under pressure of robust U.S. and U.N. sanctions, DPRK has increasingly relied on illicit activities, including cybercrime, to generate revenue for its WMD and ballistic missile programs. In particular, the United States is deeply concerned about DPRK's malicious cyber activities. DPRK has the capability to conduct disruptive and harmful cyber activity that is wholly inconsistent with the growing international consensus on what constitutes responsible State behavior in cyberspace. [Exhibit 174, p. 1]

(U) According to Annex I of the April 14, 2020 joint cyber threat advisory, the Office of the Director of National Intelligence's Annual Worldwide Threat Assessments of the U.S. IC noted in 2019 that DPRK poses a significant cyber threat to financial institutions, remains a cyber-espionage threat, and retains the ability to conduct disruptive cyber-attacks. DPRK continues to use cyber capabilities to steal more than $1.1 billion from financial institutions across the world—including a successful cyber heist of an estimated $81 million from Bangladesh Bank. [Exhibit 174, p. 9]

(U) According to an April 13, 2022 FBI Letterhead Memorandum (LHM) to OFAC, an FBI investigation into the malicious cyber activity of the DPRK dubbed in open source as LAZARUS GROUP* has revealed that ETH address 0x098B716B8Aaf21512996dC57EB0615e2383E2f96

("E2f96")[146] is a hacker-controlled digital currency address used by the LAZARUS GROUP*. [Exhibit 169, p. 1]

(U//~~FOUO~~) [redacted] [Exhibit 153, pp. 10–11]

(U) According to a June 29, 2022 Elliptic,[147] blogpost, "on the morning of June 24, 2022 over $100 million in crypto assets was stolen from Horizon Bridge–a service that allows assets to be transferred between the Harmony blockchain and other blockchains. Our analysis of the hack and the subsequent laundering of the stolen crypto assets also indicates that it is consistent with activities of the LAZARUS GROUP*. Although no single factor proves the involvement of LAZARUS GROUP*, in combination they suggest the group's involvement:

- The LAZARUS GROUP* has perpetrated several large cryptocurrency thefts totaling over $2 billion, and has recently turned its attention to DeFi services such as cross-chain bridges. For example, the group is believed to be behind the $540 million hack of Ronin Bridge.
- The theft was perpetrated by compromising the cryptographic keys of a multi-signature wallet–likely through a social engineering attack on Harmony team members. Such techniques have frequently been used by the LAZARUS GROUP*.
- The stolen crypto assets included ETH, USDT, WBTC and BNB. The thief immediately used Uniswap — a decentralized exchange (DEX) — to convert the Ethereum-based assets into a total of 85,837 ETH. This is a common laundering technique used to avoid seizure of stolen assets.
- The regularity of the deposits into Tornado Cashover extended periods of time suggests that an automated process is being used. We have observed very similar programmatic laundering of funds stolen from the Ronin Bridge, which has been attributed to LAZARUS GROUP*, as well as a number of other attacks linked to the group." [Exhibit 225, pp. 1–3]

(U//~~FOUO~~) According to blockchain analysis conducted by OFAC [redacted][148] **TORNADO CASH** received stolen funds from at least one additional LAZARUS GROUP* virtual currency heist beyond the ***Sky Mavis-Ronin Bridge Heist***:

- U.S. company Harmony Heist, aka Harmony Protocol Exploit, June 23, 2022:
  - On June 23, 2022, virtual currency address 0x58F4BACcb411ACef70A5f6DD174Af7854fc48Fa9 sent

[146] (U) "2f96" was added to the LAZARUS GROUP* SDN List entry as an identifying feature on April 14, 2022. [Exhibit 170, p. 1]
[147] (U) According to its website, Elliptic provides blockchain analytics for financial crime compliance. [Exhibit 24, p.
[148] (U//~~FOUO~~) [redacted] [Exhibit 27, p. 4]

0x0d043128146654C7683Fbf30ac98D7B2285DeD00 a total of 41,562 ETH in eight transactions.

- Between June 23–24, 2022, virtual currency address 0x9E91ae672E7f7330Fc6B9bAb9C259BD94Cd08715 sent 0x0d043128146654C7683Fbf30ac98D7B2285DeD00 a total of 31,207 ETH in 10 transactions.
- On June 23, 2022, virtual currency address 0xF50B2077d40830b2AC77f9147c65DD5E8D5b8557 sent 0x0d043128146654C7683Fbf30ac98D7B2285DeD00 a total of 0.99 ETH in two transactions.
- On June 27, 2022, 0x0d043128146654C7683Fbf30ac98D7B2285DeD00 sent 0x1Ec6F83b55C3F4CeFc630442716872BA15f16430 a total of 18,036.3 ETH in one transaction.
- On June 27, 2022 0x1Ec6F83b55C3F4CeFc630442716872BA15f1 6430 sent:
  - 6,009 ETH to 0x1Ec6F83b55C3F4CeFc630442716872BA15f16430;
  - 6,012 ETH to 0x432A9Cb4353bed67EC5351734d4a44C0826847Ae, and;
  - 6,012 ETH to 0x4507AclbdF4Ae5E61ffceC3A9AEDA312E2505970
- On June 27, 2022, 0x1Ec6F83b55C3F4CeFc630442716872BA15f1 6430 sent 6,000 ETH to **TORNADO CASH**.
- On June 27, 2022, 0x432A9Cb4353bed67EC5351734d4a44C0826847Ae sent 6,000 ETH to **TORNADO CASH**.
- On June 27, 2022, 0x4507AclbdF4Ae5E61ffceC3A9AEDA312E2505970 sent 6,000 ETH to **TORNADO CASH**. [Exhibit 164, pp. 2–3]

(U//~~FOUO~~) As described by Exhibit 145 and Exhibit 159, LAZARUS GROUP* carried out a March 2022 cyber heist of $620 million worth of virtual currency. As described by Exhibit 113, LAZARUS GROUP* is an agency, instrumentality, or entity controlled by the GONK*. As described in Exhibit 164 and Exhibit 225, DPRK carried out the Harmony heist and **TORNADO CASH** facilitated the laundering of funds derived from the heist. As described by Exhibit 168 and Exhibit 174, the GONK* has used laundered proceeds of virtual currency thefts to support its WMD and ballistic missile programs. [redacted] **TORNADO CASH** facilitated the laundering of proceeds from the March 2022 cyber heist. Therefore, OFAC assesses that **TORNADO CASH** has provided material support to the GONK*.

(U//~~FOUO~~) Additional information to support OFAC's designation of **TORNADO CASH** is available in the classified addendum to this memorandum.

VI. (U) ADDITIONAL INFORMATION

(U//~~FOUO~~) According to blockchain analysis conducted by OFAC [redacted] **TORNADO CASH** also laundered funds derived from the U.S. company Nomad Heist in August 2022 this heist has not been publicly attributed to any specific actor:

- On August 2, 2022, 0xC9943f94142D81790eCf8EEE2C879d47730cf599 sent:
  - 2,580 ETH to 0x8d5DEe51D984809D83Fe7E474755A15686121124 in two transactions.

  - 1,003 ETH to 0xbC09E7aD2adbla2D2aFC403514287AdD5fC10B9F in two transactions.
  - 1,205 ETH to 0x7a98B3F0d6e2907594Da0D97529C5cc678dFa308 in two transactions.
- On August 2, 2022, 0x8d5DEe51D984809D83Fe7E474755Al5686121124 sent 2,500 ETH to **TORNADO CASH** in 25 transactions.
- On August 2, 2022, 0xbC09E7aD2adbla2D2aFC403514287AdD5fC10B9F sent 1,000 ETH to **TORNADO CASH** in 10 transactions.
- On August 2, 2022, 0x7a98B3F0d6e2907594Da0D97529C5cc678dFa308 sent 1,200 ETH to **TORNADO CASH** in 12 transactions. [Exhibit 164, p. 2–3]

(U//~~FOUO~~) According to data [redacted], on August 2, 2019, **TORNADO CASH** received transactions worth a combined total of approximately $7 billion between its founding and August 3, 2022. [Exhibit 164, p. 3]

(U) OFAC conducted blockchain analysis of three heists that laundered funds through **TORNADO CASH**:

- Sky Mavis Ronin Bridge Heist: $455,594,329.
- Nomad Bridge Heist: approximately $7.8 million
- Harmony Heist: approximately: $96 million [Exhibit 207, pp. 2–5]

(U) According to an April 15, 2022 CoinDesk article, "Tornado Cash said Friday [April 15, 2022] "it is using a tool developed by compliance firm Chainalysis to block crypto wallets sanctioned by OFAC. However, the blockade only applies to the user-facing DApp, not the underlying smart contract," one of the protocol's founders later tweeted. [Tornado Cash], which claims to defend people's financial privacy, has often been used to obfuscate the trail of crypto obtained through hacks. The protocol's founder has previously said it is "technically impossible" to enforce sanctions on decentralized protocols like Tornado Cash. "There's not much we can do," he said in a March 2022 interview." [Exhibit 166, pp. 2–3]

(U) According to the website of **TORNADO CASH**, accessed via the Wayback Machine, the Tornado Cash Trusted Setup Ceremony had a searchable database of participants. OFAC queried this database [redacted] for **TORNADO CASH** founders Roman Storm, Roman Semenov, and Alexey Pertsev, and identified that each was named in the database, indicating that they had been participants in the Trusted Setup Ceremony. [Exhibit 71, pp. 1–3]

(U//~~FOUO~~) As described below, because cryptocurrencies use a ledger that can be viewed by anyone, users of cryptocurrencies may have concerns regarding their privacy that are distinct from those of users of traditional financial services. Cryptocurrency mixing services, such as those offered by **TORNADO CASH**, purport to be among the efforts to respond to such privacy concerns.

(U) According to a 2019 Thomson Reuters Practical Law Practice Note, "some blockchain technology features can help mitigate or cater to privacy concerns, such as using encryption and verifying data integrity. However, blockchain technology's distributed peer-to-peer network architecture often places it at odds with the traditional notion of centralized controller-based data

processing. This disconnect can make it difficult to reconcile current data protection laws with blockchain's other core elements, such as the lack of centralized control, immutability, and perpetual data storage." [Exhibit 104, p. 3]

(U) According to the same 2019 Practical Law Practice Practice Note, "blockchains, including many public blockchains that support popular cryptocurrencies, tout anonymity or at least some level of privacy by using public-private key pair encryption. These asymmetric encryption systems leverage the mathematical relationship between the public and private keys in a particular pair; record public keys on the blockchain implementation; do not typically record public key owner data or other similar personal information; and leave users to retain and protect their own private keys." [Exhibit 104, p. 3]

(U) According to the same 2019 Practical Law Practice Practice Note, "some blockchain enthusiasts claim that using public-private key encryption preserves anonymity and privacy. This is a relatively simplistic view of personal information because methods exist for linking individuals to public keys by analyzing blockchain transactions and other publicly available data. Some businesses offer services to identify individuals using their public keys, blockchain transactions, and other available data. Better practice treats public keys as tokenizations of personal information from a privacy perspective instead of anonymized data, because they correspond to an individual and reidentification becomes possible in some circumstances. Reidentification risks and related concerns have led some blockchains, including privacy-focused cryptocurrencies, to try to reduce the risk of identifying individual participants by implementing various mitigation strategies to protect transaction and other data and introducing alternative cryptographic approaches." [Exhibit 104, p. 4]

EXHIBITS LIST

Exhibit 1: (U) Website of CoinDesk, "What is Tokenomics and Why is it Important?" accessed October 1, 2022, available at: https://www.coindesk.com/learn/what-is-tokenomics-and-why-is-it-important/. (U).

Exhibit 2: (U) Executive Order 13551 of August 30, 2010, "Blocking Property of Certain Persons With Respect to North Korea," Vol. 75 No. 169. (U).

Exhibit 3: (U) [redacted] (U/~~LES~~).

Exhibit 4: (U) Website of Tornado Cash, "Torn," archived version from June 17, 2022, accessed via The Wayback Machine, available at: https://web.archive.org/web/20220617060943/https://docs.tornado.cash/general/torn (U).

Exhibit 5: (U) Website of Tornado Cash, "Staking," archived version from April 20, 2022, accessed via The Wayback Machine, available at: https://web.archive.org/web/20220420103225/https://docs.tornado.cash/general/staking (U).

Exhibit 6: (U) Website of CoinDesk, "Tornado Cash Co-Founder Says the Mixer Protocol is Unstoppable," January 25, 2022, accessed August 22, 2022, available at: www.coindesk.com/tech/2022/01/25/tornado-cash-co-founder-says-the-mixer-protocol-is-unstoppable/ (U).

Exhibit 7: (U) Website of Decrypt.co, "Tornado Cash Ethereum Token Down 50% After Sanctions," August 12, 2022, accessed August 22, 2022, available at: https://decrypt.co/107382/tornado-cash-ethereum-token-down-50-after-sanctions (U).

Exhibit 8: (U) Website of Dune, "Tornado Cash," [redacted] available at: dune.com/poma/tornado-cash_1 (U).

Exhibit 9: (U) Website of Etherscan, "Address 0x4e7B3769921C8DFBdb3d1B4c73558db079A180c7, [redacted] vailable at: https://etherscan.io/address/0x4e7b3769921c8dfbdb3d1b4c73558db079a180c7 (U).

Exhibit 10: (U) Website of Etherscan, "TORN Token," [redacted] available at: https://etherscan.io/token/0x77777feddddffc19ff86db637967013e6c6a116c#balances (U).

Exhibit 11: (U) Website of CoinMarket Cap, "Russian Ransomware Attacker Extradited to U.S. from Netherlands, Tornado Cash Dev Still Isolated," August 19, 2022, [redacted] available at: https://coinmarketcap.com/alexandria/article/russian-ransomware-attacker-extradited-to-us-from-netherlands-tornado-cash-dev-still-isolated (U).

Exhibit 12: (U) Website of BTC Geek, "Write for Us," [redacted] available at: https://btcgeek.com/write-for-us. (U).

Exhibit 13: (U) Website of Crunchbase, "Roman Semenov," [redacted] available at: www.crunchbase.com/person/roman-semenov (U).

Exhibit 14: (U) Website of Open Zeppelin, "OpenZeppelin Contracts," [redacted] available at: https://openzeppelin-contracts/Proxy.sol (U).

Exhibit 15: (U) Website of Medium, "Tornado Cash Introduces Arbitrary Amounts & Shielded Transfers," December 15, 2021, available at: https://tornado-cash.medium.com/tornado-cash-introduces-arbitrary-amounts-shielded-transfers-8df92d93c37c. (U).

Exhibit 16: (U) Website of TechTarget, "User Interface," [redacted] available at: www.techtarget.com/searchapparchitecture/definition/user-interface-UI (U).

Exhibit 17: (U) Website of SPDX, "Overview," [redacted] available at: https://spdx.dev/about/ (U).

Exhibit 18: (U) Website of Cointelegraph, "Tornado Cash community fund multisignature wallet disbands amid sanctions," August 15, 2022, available at: https://cointelegraph.com/news/tornado-cash-community-fund-multi-signature-wallet-disbands-amid-sanctions (U).

Exhibit 19: (U) Website of Immunefi, "About," [redacted] available at: https://immunefi.com/about/. (U).

Exhibit 20: (U) Website of Internet Archive, "About," [redacted] available at: https://archive.org/about/ (U).

Exhibit 21: (U) Website of Investopedia, "What Crypto Users Need to Know: The ERC20 Standard," updated August 24, 2021 [redacted] available at: www.investopedia.com/tech/why-crypto-users-need-know-about-erc20-token-standard/ (U).

Exhibit 22: (U) Website of Cointelegraph, "What is a crypto airdrop, and how does it work" July 14, 2022, accessed August 18, 2022 available at:

https://cointelegraph.com/news/what-is-a-crypto-airdrop-and-how-does-it-work (U).

Exhibit 23: (U) Website of Cointelegraph, "About," accessed April 1, 2022, available at: https://cointelegraph.com/about/ (U).

Exhibit 24: (U) Website of the Elliptic, "Our Story," [redacted] available at: https://www.elliptic.co/our-story. (U).

Exhibit 25: (U) Website of Cointelegraph, "Understanding Staking Pools: The Pros and cons of staking cryptocurrency," May 9, 2022, accessed August 25, 2022, available at: https://cointelegraph.com/explained/understanding-staking-pools-the-pros-and-cons-of-staking-cryptocurrency (U).

Exhibit 26: (U) Website of Chainalysis, "About Us," [redacted] available at: www.chainalysis.com/company/ (U).

Exhibit 27: (U~~//FOUO~~) [redacted] (U~~//FOUO~~)

Exhibit 28: (U) Website of SPDX MIT, "MIT License," [redacted] available at: https://spdx.org/licenses/MIT.html (U).

Exhibit 29: (U) Website of Etherscan, "About Etherscan," [redacted] available at: https://etherscan.io/aboutus (U).

Exhibit 30: (U) Website of Etherscan, "Transaction Details 0xab," [redacted] available at: https://etherscan.io/tx/0xab822174f2b6177867d53eeea05ed7e80965b9b412f42f5a55674fe900399019 (U)

Exhibit 31: (U) Website of OKX, "Contact Us," [redacted] available at: www.okx.com/contactu-us.html (U).

Exhibit 32: (U) Securities Exchange Commission, "1inch LTD," accessed August 25, 2022, available at: https://sec.report/CIK/0001830516 (U).

Exhibit 33: (U) Website of Crunchbase, "About Crunchbase," July 28, 2017, available at: www.about.crunchbase.com/about-us/ (U).

Exhibit 34: (U) Website of Bitcoin.com, "Tornado Cash Governance Token TORN Shudders More than 57% Since the US government Ban," August 13, 2022, [redacted] available at: news.bitcoin.com/tornado-cash-governance-token-torn-shudders-more-than-57-since-the-us-government-ban/ (U).

Exhibit 35: (U) Website of Decrypt, "What is 1inch Exchange? Beginners Guide," June 23, 2021, accessed October 7, 2022, available at: https://decrypt.co/resources/1inch-dex-aggregator-decentralized-exchanges (U).

Exhibit 36: (U) Website of Etherscan, "Address 0x5efda50f22d34F262c29268506C5Fa42cB56A1Ce," [redacted] vailable at: https://etherscan.io/address/0x5efda50f22d34f262c29268506c5fa42cb56a1ce (U).

Exhibit 37: (U) Website of Binance. "TORN," [redacted] available at: www.binance.com/en/trade/TORN_BUSD?_from=markets&theme=dark&type=spot (U).

Exhibit 38: (U) Website of Github, "Gnosis Chain / media-kit," [redacted] available at: https://github.com/gnosischain/media-kit. (U).

Exhibit 39: (U) Website of Medium, "Tornado.cash Trusted Setup Ceremony," May 1, 2020, available at: https://tornado-cash.medium.com/tornado-cash-trusted-setup-ceremony-b846e1e00be1 (U).

Exhibit 40: (U) Website of Altcoin Buzz, "About Altcoin Buzz," [redacted] 2022, available at: https://www.altcoinbuzz.io/about-altcoin-buzz/. (U).

Exhibit 41: (U) Website of Medium, "What is Medium?," accessed April 29, 2022, available at: www.medium/com/about?autoplay=1 (U).

Exhibit 42: (U) Website of Kharon, "Developer of Sanctioned Crypto Mixer Arrested, Was Employed by Company Linked to Russia's FSB," August 24, 2022, available at: https://brief.kharon.com/updates/ceo-of-sanctioned-crypto-mixer-arrested-was-employed-by-company-linked-to-russia-s-fsb/ (U).

Exhibit 43: (U) Website of Kharon, "About Kharon," [redacted] available at: www.kharon.com/#kharon-company (U).

Exhibit 44: (U) Website of the Department of the Treasury, "Treasury Sanctions Russian Federal Security Service Enablers," June 11, 2018, available at: https://home.treasury.gov/news/press-releases/sm0410 (U).

Exhibit 45: (U) Executive Order 13757 of December 28, 2016, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," 82 Fed. Reg. 1 (January 3, 2017) (U).

Exhibit 46: (U) U.S. Department of State, Press Release, "U.S. Sanctions and Other Measures Imposed on Russia in Response to Russia's Use of Chemical

Weapons," March 2, 2021, available at: www.state.gov/u-s-sanctions-and-other-measures-imposed-on-russia-in-response-to-russias-use-of-chemical-weapons/ (U).

Exhibit 47: (U) Website of Investopedia, "Hot Wallet," [redacted] available at: investopedia.com/terms/h/hot-wallet.asp. (U).

Exhibit 48: (U) Website of GitHub, "Tornado Repositories," [redacted] available at: https://github.com/tornado-repositories (U).

Exhibit 49: (U) Website of CoinTelegraph, "DeFI Staking a Beginners Guide to proof-of-Stake Coins,"," accessed October 24, 2022, available at: https://cointelegraph.com/defi-101/defi-staking-a-beginners-guide-to-proof-of-stake-pos-coins#:~:text=Staking%20pools%20allow%20people%20to,the%20amount%20on%20their%20holdings. (U).

Exhibit 50: (U) Website of Ethereum, "Introduction to Ethereum Governance," August 29, 2022, [redacted] available at: https://ethereum.org/en/governance/ (U).

Exhibit 51: (U) Website of Blockchain Council, "What is Dai?," May 13, 2022, [redacted] available at: https://www.blockchain-council.org/dao/what-is-dai/. (U).

Exhibit 52: Website of DeCrypt, "What is Compound?" April 20, 2020, accessed October 6, 2022, available at: https://decrypt.co/resources/compound-defi-ethereum-explained-guide-how-to. (U).

Exhibit 53: (U) [redacted]
(U//~~FOUO~~).

Exhibit 54: (U) Website of the Department of the Treasury, Press Releases, "Treasury Takes Robust Actions to Counter Ransomware," September 21, 2021, available at: https://home.treasury.gov/news/press-releases/jy0364. (U).

Exhibit 55: (U) Website of Vitalik, "How do Trusted Setups Work?" March 14, 2022, [redacted] available at: vitalik.ca/general/2022/03/14/trusted.html (U).

Exhibit 56: (U) Website of Cryptotimes, "Velodrome Regains $350k Stolen by its Developer Gabagool," August 15, 2022, [redacted] available https://www.cryptotimes.io/velodrome-regains-350k-stolen-by-its-developer-gabagool/ (U).

Exhibit 57: (U) Website of Coindesk, "Cloning Tornado Cash Would Be Easy, but Risky," accessed September 16, 2022, available at: www.coindesk.com/tech/2022/08/10/cloning-tornado-cash-would-be-easy-but-risky/ (U).

Exhibit 58: (U) Website of Ethereum, "Ethereum Accounts," [redacted] available at: https://ethereum.org/en/developers/docs/accounts/ (U).

Exhibit 59: (U) Chainalysis, "Dissecting the DAO: Web3 Ownership is Surprisingly Concentrated," [redacted] available at: https://blog.chainalysis.com/reports/web3-daos-2022/ (U).

Exhibit 60: (U) Website of Medium, "How to Stay Anonymous with Tornado.cash and similar solutions, [redacted] available at: https://tornado-cash.medium.com/how-to-stay-anonymous-with-tornado-cash-and-similar-solutions-efdecdbd7d37 (U).

Exhibit 61: (U) Website of Medium, "Tornado.Cash Governance Proposal," archived version from December 18, 2020 accessed via The Wayback Machine, available at: https://web.archive.org/web/20220808144451/https://tornado-cash.medium.com/tornado-cash-governance-proposal-a55c5c7d0703#bf59 (U).

Exhibit 62: (U) Website of Coin Center, "How does Tornado Cash work?" August 25, 2022, [redacted] available at: www.coincenter.org/education/advanced-topics/how-does-tornado-cash-work/ (U).

Exhibit 63: (U) Website of Chainalysis, "Crypto Mixers and AML Compliance," August 23, 2022, [redacted] vailable at: https://blog.chainalysis.com/reports/crypto-mixers/ (U).

Exhibit 64: (U) Website of Tornado Cash, "How Tornado Cash Works," archived version from February 18, 2022, accessed via The Wayback Machine [redacted], available at: https://web.archive.org/web/20220218214742/https://tornado.cash/ (U).

Exhibit 65: (U) Website of the Department of the Treasury, Press Releases, "Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange," November 8, 2021, available at: https://home.treasury.gov/news/press-releases/jy0471

Exhibit 66: (U) Website of Investopedia, "Application Programming Interface (API)," [redacted] available at: investopedia.com/terms/a/application-programming-interface.asp. (U).

Exhibit 67: (U) Website of Snapshot, "Home-Snapshot," [redacted] available at: https://docs.snapshot.org (U).

Exhibit 68: (U) Website of Investopedia, "Atomic Swap Definition," August 14, 2022, [redacted] available at: https://www.investopedia.com/terms/a/atomic-swaps.asp#:~:text=An%20atomic%20swap%20is%20an,give%20token%20owners%20total%20control. (U).

Exhibit 69: (U) Website of Medium, "What Are Cliffs And Vesting, And Why Do They Matter?" December 9, 2021, accessed September 13, 2022, available at: https://medium.com/@playSIPHER/what-are-cliffs-and-vesting-and-why-do-they-matter-8c21eec37c99 (U).

Exhibit 70: (U) Website of Medium, "What's Up Tornado – Some Digging on Tornado Cash Decision Making," September 6, 2021, archived version from August 8, 2022, accessed via The Wayback Machine on September 9, 2022, available at: https://web.archive.org/web/20220808144523/https://wutornado.medium.com/whats-up-tornado-some-digging-on-tornadocash-decision-making-8db64014112 (U).

Exhibit 71: (U) Website of Tornado Cash, "Ceremony," archived version from August 5, 2020, accessed via The Wayback Machine [redacted] available at https://web.archive.org/web/20200805042602/https://ceremony.tornado.cash/ (U).

Exhibit 72: (U) Website of FIOD "Arrest of suspected developer of Tornado Cash," August 8, 2022, available at: https://www.fiod.nl/arrest-of-suspected-developer-of-tornado-cash/ (U).

Exhibit 73: (U) Website of Investopedia, "USD Coin." September 27, 2022, [redacted] available at: https://www.investopedia.com/usd-coin-5210435. (U).

Exhibit 74: (U) Website of Github, "Tornado-repositories/tornado-core Commits on March 24, 2022," [redacted] available at: https://github.com/tornado-repositories/tornado-core/commits/master (U).

Exhibit 75: (U) Website of Medium "What is the xDai Chain and Why Should I Try It?" March 3, 2021, accessed October 6, 2022, available at: https://medium.com/mycrypto/what-is-the-xdai-chain-and-why-should-i-try-it-40f539732fb4

Exhibit 76: (U) Website of DeCrypt, "What is Wrapped Bitcoin?" March 17, 2022, accessed October 6, 2022, available at: https://decrypt.co/resources/what-is-wbtc-explained-bitcoin-ethereum-defi. (U).

Exhibit 77: (U) Website of Dune, "Tornado Cash Fees V04" [redacted] available at: https://dune.come/queries/671343/124581 (U).

Exhibit 78: (U) Website of MakeUseOf, "What is Software Forking," July 7, 2021, [redacted] available at: www.makeuseof.com/what-is-software-forking/ (U).

Exhibit 79: (U) Website of Dune, "Introduction to Dune/Dune Docs," [redacted] available at: https://docs.dune.com (U).

Exhibit 80: (U) Website of Github, "Github's Products" [redacted] available at: https://docs.github.com/en/get-s github/githubs-products (U).

Exhibit 81: (U) Website of CoinDesk, "How Bitcoin Mixers Work and Why People Use BitcoinMixers," January 18, 2022, [redacted] available at: https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used/ (U).

Exhibit 82: (U) Website of Council on Foreign Relations, "About CFR," [redacted] available at: cfr.org/about. (U).

Exhibit 83: (U) Website of GitHub, "openzeppelin-contracts / contracts / proxy," [redacted] available at: https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/proxy/Proxy.sol (U).

Exhibit 84: (U) Website of SPDX, "SPDX License List," [redacted] available at: https://sodx.org/licenses/ (U).

Exhibit 85: (U) Website of Forbes, "What is AVAX," September 16, 2022 accessed October 6, 2022, available at: https://www.forbes.com/sites/qai/2022/09/16/avalanche-crypto-news-whats-going-on-with-the-scandal-surrounding-avax/?sh=66903beb6e8b

Exhibit 86: (U) Website of GitHub, "Tornado Repositories/Tornado Classic UI," [redacted] available at: https://github.com/tornado-repositories/tornado-classic-ui/blob/master/LICENSE (U).

Exhibit 87: (U) Website of Medium, "Decentralizing TornadoCash: The Launch of TornadoFund and the Path Towards TornadoDAO," July 1, 2020, accessed September 21, 2022, available at:

https://medium.com/@Tornado_Fund/decentralizing-tornadocash-the-launch-of-tornado-fund-and-the-path-towards-tornadodao-a6d4ffc6c800 (U).

Exhibit 88: (U) Website of OpenZeppelin, "Explore using OpenZeppelin," [redacted] vailable at: https://docs.openzeppelin.com (U).

Exhibit 89: (U) Website of Crypto.com, "Crypto Tokens vs Coins – what's the difference? June 20, 2022 [redacted] available at: https://crypto.com/university/crypto-tokens-vs-coins-difference

Exhibit 90: (U) Website of Etherscan, "Token Torn Token," [redacted] available at: https://etherscan.io/token/0x77777feddddffc19ff86db637967013e6c6a116c#balances. (U)

Exhibit 91: (U) Website of Binance, [redacted] vailable at: https://www.binance.com/en. (U).

Exhibit 92: (U) Website of Binance, "List of Supported Assets- Binance.US, [redacted] available at: https://support.binance.us/hc/en-us/articles/360049417674-List-of-Supported-Assets. (U).

Exhibit 93: (U) Website of Coinbase, "Compound Dai," [redacted] available at: https://www.coinbase.com/price/compound-dai?__cf_chl_f_tk=D5VVEgmSWkF1fT7uFKgMSkvkGu8IEMSELpOHdXsjtR4-1664657609-0-gaNycGzNCZE#CompoundDaiCDAI. (U).

Exhibit 94*: (U) Website of Tech Target, "Code Base," [redacted] available at: www.techtarget.com/whatis/definition/codebase-code-base (U).

Exhibit 95: (U) Website of Tech Target, "Source Code," [redacted] available at: www.techtarget.com/searchapparchitecture/definition/source-code (U).

Exhibit 96: (U) Website of Etherscan, "Contract 0x58E8dCC13BE9780fC42E8723D8EaD4CF46943dF2," [redacted] available at: https://etherscan.io/address/0x58E8dCC13BE9780fC42E8723D8EaD4CF46943dF2 (U).

Exhibit 97: (U) Website of CoinDesk, "Custodial Wallets vs Non-Custodial Crypto Wallets," March 9, 2022, accessed September 22, 2022, available at: www.coindesk.com/learn/custodial-wallets-vs-non-custodial-crypto-wallets/ (U).

Exhibit 98: (U) Website of Forbes, "Leaked 'Tai Chi' Document Reveals Binance's Elaborate Scheme To Evade Bitcoin Regulators," October 29, 2020, accessed September 22, 022 available at: www.forbes.com/sites/michaeldelcastillo/2020/10/29/leaked-tai-chi-document-reveals-binances-elaborate-scheme-to-evade-bitcoin-regulators/?sh=3eff18812a92 (U).

Exhibit 99: (U) Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," April 1, 2015. (U).

Exhibit 100: (U) Executive Order 13722, "Blocking the Property of the Government of North Korea and the Workers' Party of Korea, and Prohibiting Certain Transactions With Respect to North Korea," March 18, 2016. (U)

Exhibit 101: (U//~~FOUO~~) OFAC Memorandum for Record, "Analysis of TORNADO CASH Addresses and Contracts." (U//~~FOUO~~)

Exhibit 102: (U) Website of Investopedia, "Tether (USDT): Meaning and Uses for Tether Crypto Explained, May 12, 2022, [redacted] available at: https://www.investopedia.com/terms/t/tether-usdt.asp. (U).

Exhibit 103: (U) Website of Ethereum, "Intro to Ethereum," [redacted] available at: ethereum.org/en/developers/docs/intro-to-ethereum/. (U).

Exhibit 104: (U) Thompson Reuters "Blockchain technology: Data Privacy Issues and Potential Mitigation Strategies," Resource ID: W-021-8235. (U).

Exhibit 105: (U) Website of CoinMarket Cap, "Glossary – Annual Percentage Yield," [redacted] vailable at: https://coinmarketcap.com/alexandria/glossary/annual-percentage-yield-apy. (U).

Exhibit 106: (U//~~FOUO~~) [redacted] (U//~~FOUO~~).

Exhibit 107: (U) Website of Ethereum, "Transactions," [redacted] available at: ethereum.org/en/developers/d

Exhibit 108: (U) Website of Certik, "What is Blockchain Analysis? – Blog," [redacted] available at: certik.com/resources/blog/what-is-blockchain-analysis. (U).

Exhibit 109: (U) Website of Certik, "About," [redacted] available at: certik.com/company/about. (U).

Exhibit 110: (U) Website of Council on Foreign Relations, "Cryptocurrencies, Digital Dollars, and the Future of Money," updated September 24, 2021, [redacted] Available at: https://www.cfr.org/backgrounder/cryptocurrencies-digital-dollars-and-future-money?gclid=EAIaIQobChMI-b_uvai6-gIVk4vICh1BLAqHEAAYASAAEgLz%E2%80%A6. (U).

Exhibit 111: (U) Website of Ethereum, "ERC-20 Token Standard," [redacted] Available at: ethereum.org/en/developers/docs/standards/tokens/erc-20/. (U).

Exhibit 112: (U) Website of the Department of the Treasury, Press Releases, "Treasury Sanctions Russia-based Hydra, World's Largest Darknet Market, and Ransomware Enabling Virtual Currency Exchange Garantex," April 5, 2022. Available at: https://home.treasury.gov/news/press-releases/jy0701. (U).

Exhibit 113: (U) Website of the Department of the Treasury, Press Releases, "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups," September 13, 2019. Available at: https://home.treasury.gov/news/press-releases/sm774. (U).

Exhibit 114: (U) Website of the Department of the Treasury, Press Releases, "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats." May 6, 2022. Available at: https://home.treasury.gov/news/press-releases/jy0768. (U)

Exhibit 115: (U) Website of Cointelegraph, "What are NFT's?" accessed August 25, 2022, available at: https://cointelegraph.com/tags/nft (U).

Exhibit 116: (U) Website of Chainalysis, "Crypto Mixer Usage Reaches All-time Highs in 20222, With Nation State Actors and Cyber Criminals Contributing Significant Volume. July 14, 2022, [redacted] available at: blog.chainalysis.com/reports/crypto-mixer-criminal-volume-2022/. (U).

Exhibit 117: (U) Website of the Department of the Treasury, "Frequently Asked Questions #561," March 19, 2018, accessed September 28, 2022. Available at: https://home.treasury.gov/policy-issues/financial-sanctions/faqs/561. (U).

Exhibit 118: (U) Website of Ethereum, "Smart Contract Languages," August 22, 2022, [redacted] available at: https://ethereum.org/en/developers/docs/smart contracts/languages/#solidity. (U).

Exhibit 119: (U) Website of Tornado Cash, "jobs," [redacted] formerly available at: https:tornado.cash/jobs/solidity-engineer. (U).

Exhibit 120: (U) Website of Tornado Cash, "Introduction," [redacted] captured August 5, 2022, available at: https://web.archive.org/web/20220805205724/https://docs.tornado.cash/general/readme. (U).

Exhibit 121: (U) Website of Cointelegraph, "TORN soars 200% as Tornado.Cash's Governance token becomes tradable." February 9, 2021, accessed September 30, 2022. Available at: https://cointelegraph.com/news/torn-soars-200-as-tornado-cash-s-governance-token-becomes-tradable. (U).

Exhibit 122: (U) Website of Tornado Cash, "Community Involvement," [redacted] available at: web.archive.org/web/20220617060922/https://docs.tornado.cash/general/community-involvement. (U).

Exhibit 123: (U) Website of CoinDesk, "An Introduction to Sidechains," March 7, 2022, accessed September 30, 2022, available at: coindesk.com/learn/an-introduction-to-sidechains/. (U).

Exhibit 124: (U) Website of Forbes, "What is Tether? How Does it Work?" accessed September 30, 2022, available at: forbes.com/advisor/investing/cryptocurrency/what-is-tether-usdt/. (U).

Exhibit 125: (U) Website of Decrypt, "What is Wrapped Bitcoin?" May 17, 2022, accessed September 30, 2022. Available at: decrypt.co/resources/what-is-wbtc-explained-bitcoin-ethereum-defi. (U).

Exhibit 126: (U) Website of CoinMarketCap, "What is Binance Smart Chain?" [redacted] available at: coinmarketcap.com/alexandria/article/what-is-binance-smart-chain. (U).

Exhibit 127: (U) Website of CoinMarket Cap, "About CoinMarketCap," [redacted] available at: https://coinmarketcap.com/about/. (U).

Exhibit 128: (U) Website of Investopedia, "About Us," [redacted] available at: www.investopedia.comn/about-us-5093223 (U).

Exhibit 129: (U) Website of Investopedia, "Polygon (MATIC)," [redacted] 2022, available at: https://www.investopedia.com/polygon-matic-definition-5217569#:~:text=Polygon (MATIC) is a cryptocurrency,such as Coinbase or Kraken. (U).

Exhibit 130: (U) National Institute of Standards and Technology, "Blockchain Technology Overview," October 2018. (U).

Exhibit 131: (U) Website of Medium "Avalanche Mainnet is Live," October 15, 2022, accessed September 30, 2022, available at: medium.com/avalancheavax/avalanche-mainnet-is-live-c2101c82ce10. (U).

Exhibit 132: (U) Website of Tornado Cash, "Circuits," [redacted] available at: web.archive.org/web/20220617060935/https://docs.tornado.cash/tornado-cash-classic/circuits. (U).

Exhibit 133: (U) Website of Zcash, "What are ZK-SNARKs?" [redacted] available at: https://z.cash/technology/zksnarks/. (U).

Exhibit 134: (U) Website of Tornado Cash, "Connect your wallet" [redacted] available at: web.archive.org/web/20220617060938/https://docs.tornado.cash/tornado-cash-classic/how-to-connect-your-wallet. (U).

Exhibit 135: (U) Website of Tornado Cash, "Deposit & Withdraw -Tornado Cash," [redacted] available at: web.archive.org/web/20220619102910/https://docs.tornado.cash/tornado-cash-classic/deposit-withdraw. (U).

Exhibit 136: (U) Website of Tornado Cash, "Fund & Withdraw on Nova," [redacted] available at: web.archive.org/web/20220617060939/https://docs.tornado.cash/tornado-cash-nova/fund-and-withdraw-on-nova. (U).

Exhibit 137: (U) Website of Tornado Cash, "Shielded transfers on Nova – Tornado.Cash," [redacted] available at: web.archive.org/web/20220617060938/https://docs.tornado.cash/tornado-cash-nova/shielded-transfers-on-nova. (U).

Exhibit 138: (U) Website of Tornado Cash, "Anonymity Mining," [redacted] available at: web.archive.org/web/20220617060938/https://docs.tornado.cash/tornado-cash-classic/anonymity-mining. (U).

Exhibit 139: (U) Website of Tornado Cash, "How to Become a Relayer?" [redacted] available at: web.archive.org/web/20220609181519/https://docs.tornado.cash/general/how-to-become-a-relayer. (U).

Exhibit 140: (U) Website of Coinbase, "RPC Node, " [redacted] available at: https://help.coinbase.com/en/coinbase/getting-started/crypto-education/glossary/rpc-node. (U).

Exhibit 141: (U) Website of Uniswap, "Introducing Uniswap V3," March 23, 2021, [redacted] available at: uniswap.org/blog/uniswap-v3. (U).

Exhibit 142: (U) Website of BTCGeek, "How to Buy TORN Token from Tornado. ETH's most Trusted Privacy Protocol" February 9, 2021, [redacted] vailable at: https://btcgeek.com/buy-torn-token-tornado/. (U).

Exhibit 143: (U) Website of Medium, "Introducing ppTORN: an Auto-compounding strategy for Tornado.cash $TORN governance Staking. April 30, 2022, available at: medium.com/powerpool/introducing-pptorn-an-auto-compounding-strategy-for-tornado-cash-torn-governance-staking-1bd8d78e64a0. (U)

Exhibit 144: (U) Website of AltcoinBuzz, "Make 61% APY with TORN on this Platform," May 11, 2022, [redacted] available at: https://www.altcoinbuzz.io/passive-income/staking/make-61-apy-with-torn-on-this-platform/. (U).

Exhibit 145: (U) Website of Reuters, "Explainer: Ronin's $615 Million Crypto Heist," March 30, 2022, accessed April 20, 2022. Available at: https://www.reuters.com/technology/ronins-615-million-crypto-heist-2022-03-30/. (U).

Exhibit 146: (U) Website of Barron's, "Inside the $625 Million Axie Hack and What it Means for Crypto Gaming," March 30, 2022, accessed April 29, 2022 available at: https://www.barrons.com/articles/axie-infinity-hack-cryptocurrency-defi-gaming-51648671214. (U)

Exhibit 147: (U) Website of Reuters, accessed April 29, 2022, Available at: https:reuters.com/. (U).

Exhibit 148: (U) Website of Barron's, "About," accessed April 14, 2022, Available at: https://www.barrons.com/100-years-of-barrons/about

Exhibit 149: (U) Department of the Treasury, "Imposition of Sanctions Pursuant to Executive Order 13687 on January 2, 2015". (U).

Exhibit 150: (U) Website of CoinDesk, "Twitters says 'Phone Spear Phishing' Let h ackers Gain employee Credentials," Updated September 14, 2022, accessed April 14, 2022, available at: https://www.coindesk.com/markets/2020/07/31/twitter-says-phone-spear-phishing-let-hackers-gain-employee-credentials/. (U).

Exhibit 151: (U) Website of CoinDesk, "About," Accessed April 14, 2022, available at: https://www.coindesk.com/about/. (U).

Exhibit 152: (U) Website of CoinTelegraph, "What is P2P trading, and how does it work in peer-to-peer crypto exchanges?" May 16, 2022, accessed September 30, 2022, Available at: cointelegraph.com/news/what-is-p2p-trading-and-how-does-it-work-in-peer-to-peer-crypto-exchanges. (U).

Exhibit 153: (U//~~FOUO~~) [redacted] (U//~~FOUO~~).

Exhibit 154: (U) Website of Medium, "Validator Node FAQ," February 25, 2021, accessed April 29, 2022, Available at: https://medium.com/centrality/validator-node-faq-154c728bac82#:~:text=Validators are node operators who,voting in the finalization protocol. (U).

Exhibit 155: (U) Website of Gnosis, "What is Gnosis Safe? Gnosis Help Center," [redacted] available at: https://help.gnosis-safe.io/en/articles/3876456-what-is-gnosis-safe. (U).

Exhibit 156: (U) Website of Medium, "Getting to Know Third Party Validators," October 14, 2020, accessed April 29, 2022. Available at: https://medium.com/stakefish/getting-to-know-third-party-validators-79b054b44ce7 (U).

Exhibit 157: (U) Website of Ethereum, "Decentralized Autonomous Organizations," [redacted] available at: ttps://ethereum.org/en/dao/. (U).

Exhibit 158: (U) Website of CoinDesk, " This Elusive Malware Has Been Targeting Crypto Wallets for a Year," January 6, 2021, accessed April 29, 22, available at: https://www.coindesk.com/tech/2021/01/06/this-elusive-malware-has-been-targeting-crypto-wallets-for-a-year/. (U).

Exhibit 159: (U) Website of the Federal Bureau of Investigation," FBI Statement of the Attribution of Malicious Cyber Activity Posed by the Democratic People's Republic of Korea," April 14, 2022, available at: https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea. (U).

Exhibit 160: (U) Website of Tornado Cash, "FAQ," [redacted] available at: https://tornado.cash/#faq. (U)>

Exhibit 161: (U) Website of Finance Brokerage, "Crypto Mixer Tornado Cash Won't Comply With Sanctions," March 11, 2022, [redacted]

Available at: financebrokerage.com/crypto-mixer-tornado-cash-wont-comply-with-sanctions/. (U).

Exhibit 162: (U) Website of Finance Brokerage, "About Us," [redacted] 2022, available at: financebrokerage.com/about-us/ (U).

Exhibit 163: (U) Website of Bloomberg, "Crypto Funds From Ronin Breach Moved to Tornado Cash," April 4, 2022, accessed September 29, 2022, Available at: https://www.bloomberg.com/news/articles/2022-04-04/hacker-move-stolen-crypto-funds-from-ronin-breach-to-obfuscator. (U).

Exhibit 164: (U//~~FOUO~~) OFAC Memorandum for Record, "Blockchain Analysis of TORNADO CASH." August 3, 2022. (U//~~FOUO~~)

Exhibit 165: (U) Website of CoinDesk, "Tornado Cash Co-Founder Says the Mixer Protocol is Unstoppable," January 25, 2022, accessed May 4, 2022, available at: https://www.coindesk.com/tech/2022/01/25/tornado-cash-co-founder-says-the-mixer-protocol-is-unstoppable/. (U).

Exhibit 166: (U) Website of CoinDesk, "Tornado Cash Adds Chainalysis Tool for Blocking OFAC-Sanctioned Wallets from Dapp," April 15, 2022, accessed September 29, 2022, available at: coindesk.com/tech/2022/04/15/tornado-cash-adds-chainalysis-tool-for-blocking-ofac-sanctioned-wallets-from-dapp/. (U).

Exhibit 167: (U) Joint Cyber Security Advisory, "TraderTraitor: North Korean State-Sponsored APT Targets BlockChain Companies," April 18, 2022. (U).

Exhibit 168: (U) United Nations Security Council, "Letter dated 27 August 2019 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council S/2019/691" August 30, 2019. (U).

Exhibit 169: (U) Federal Bureau of Investigation, "Letterhead Memorandum 349F-CE-2200375," April 13, 2022. (U).

Exhibit 170: (U) Vol. 87, No. 82 Federal Register 25352, April 28, 2022. (U).

Exhibit 171: (U) Website of Bloomberg, "Hackers Steal about $600 Million in One of the biggest Crypto Heists," March 29, 2022, available at: https://www.bloomberg.com/news/articles/2022-03-29/hackers-steal-590-million-from-ronin-in-latest-bridge-attack#xj4y7vzkg. (U).

Exhibit 172: (U) Website of Crypto News Australia, "About Crypto News," accessed October 1, 2022, available at: https://cryptonews.com.au/about. (U).

Exhibit 173: (U) Website of CoinDesk, "Why TVL Matters in DeFi: Total Value Locked Explained," accessed September 29, 2022, available at: https: //www.coindesk.com/learn/why-tvl-matters-in-defi-total-value-locked-explained/. (U).

Exhibit 174: (U) DPRK Cyber Threat Advisory, "Guidance on the North Korean Cyber Threat," April 15, 2020. (U).

Exhibit 175: (U) Website of Immunefi, "Tornado Cash Bug Bounties," [redacted] available at: https://web.archive.org/web/20220527111152/https://immunefi.com/bounty/tornadocash/ (U).

Exhibit 176: (U) Website of Crypto News Australia, "Tornado Cash Token (TORN) Surges 94% following Bullish Protocol Updates," March 5, 2022, accessed September 30, 2022, available at: https://cryptonews.com.au/tornado-cash-token-torn-surges-94-following-bullish-protocol. (U).

Exhibit 177: (U) Website of Tornado Cash, "Tornado Cash smart contracts – Tornado.Cash" [redacted] available at: web.archive.org /web/20220617060935/https://docs.tornado.cash/general/tornado-cash-smart-contracts. (U).

Exhibit 178: (U) Chainalysis, "The 2022 Crypto Crime Report," February, 2022. (U).

Exhibit 179: (U) Attorney General's Cyber Digital Task Force, "Cryptocurrency Enforcement Framework," October, 2020. (U).

Exhibit 180: (U) Website of Reuters, "U.N. Experts point finger at North Korea for $281 million cyber theft, KuCoin likely Victim," February 29, 2021, accessed October 1, 2022, available at: https://www.reuters.com/article/us-northkorea-sanctions-cyber/u-n-experts-point-finger-at-north-korea-for-281-million-cyber-theft-kucoin-likely-victim-id%E2%80%A6. (U).

Exhibit 181: (U//~~FOUO~~) OFAC Blockchain Analysis, "Blockchain Analysis of Tornado Cash and KuCoin Theft," October 1, 2022. (U//~~FOUO~~).

Exhibit 182: (U) Website of Etherscan, "Contract 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291," [redacted] available at https://etherscan.io/address/0xA160cdAB225685dA1d56aa342Ad8841c3b53f291#code. (U).

Exhibit 183: (U Department of the Treasury, "National Money Laundering Risk Assessment," February, 2022. (U).

Exhibit 184: (U) Website of BeinCrypto, "Ethereum Name Service (ENS): Everything you Needs to Know," May 12, 2022, [redacted] available at: beincrypto.com/learn/ethereum-name-service-ens/. (U).

Exhibit 185: (U) Website of Ethereum, "Layer-2," [redacted] available at: Ethereum.org/en/layer-2/. (U).

Exhibit 186: (U) Website of Ethereum, "Sharding," [redacted] available at: Ethereum.org/en/upgrades/sharding/, (U).

Exhibit 187: (U) Website of Investopedia, "What is Altcoin," updated May 16, 2022 [redacted] available at: https://www.investopedia.com/terms/a/altcoin.asp#:~:text=Investopedia%20%2F%20Michela%20Buttignol-,What%20Is%20Altcoin%3F,from%20one%20of%20the%20two. (U).

Exhibit 188: (U) Website of Cointelegrpah, "Venture Capital financing. A Beginners Guide to VC Funding the Crypto Space." Accessed October 2, 2022, available at: https://cointelegraph.com/funding-for-beginners/venture-capital-financing-a-beginners-guide-to-vc-funding-in-the-crypto-space. (U).

Exhibit 189: (U) National Institute of Standards and Technology, "Blockchain Networks: Token Design and Management Overview," February 2021. (U).

Exhibit 190: (U) Website of CoinTelegraph, "a Beginner's Guide to the BNB Chain: The evolution of the Binance Smart Chain," accessed October 2, 2022, available at: cointelegraph.com/altcoins-for-beginners/a-beginners-guide-to-the-bnb-chain-the-evolution-of-the-binance-smart-chain. (U).

Exhibit 191: (U) Website of Investopedia, "What is Avalanche (AVAX)?" September 27, 2022, [redacted] available at: https://www.investopedia.com/avalanche-avax-definition-5217374. (U).

Exhibit 192: (U) Website of Gnosis Chain, "Developers Overview," [redacted] available at: https://docs.gnosischain.com/developers. (U).

Exhibit 193: (U) Website of CoinTelegraph. "Cryptocurrency On-Ramps and Off-Ramps, Explained," August 18, 2020, accessed October 3, 2020, available at: https://cointelegraph.com/explained/cryptocurrency-on-ramps-and-off-ramps-explained. (U).

Exhibit 194: (U) Website of Binance, "Token Lockup," [redacted] available at: https://academy.binance.com/en/glossary/token-lockup. (U).

Exhibit 195: (U) Website of Twitter, "Tornado Cash," August 23, 2019, accessed October 3, 2022, available at:

https://twitter.com/tornadocash/status/1164903335532609537. (U).

Exhibit 196: (U) Website of Decrypt, "Manifesto," Accessed October 5, 2022, available at: https://decrypt.co/manifesto . (U).

Exhibit 197: (U) Website of Immuta, "K-Anonymity: Everything You Need to Know," [redacted] vailable at: https://www.immuta.com/blog/k-anonymity-everything-you-need-to-know-2021-guide/#:~:text=What%20is%20k%2DAnonymity%3F,that%20data%20can%20be%20obscured. (U).

Exhibit 198: (U) Website of Tech Target, "Permissioned vs. permissionless blockchains: Key differences," [redacted] available at: https://www.techt [redacted] missioned-vs-permissionless-blockchains-Key-differences.

Exhibit 199: (U) Website of Harvard Law School Forum on Corporate Governance, "An Introduction to Smart Contracts and Their Potential and Inherent Limitations," May 6, 2018, [redacted] available at: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/

Exhibit 200: (U) Department of the Treasury, "National Proliferation Financing Risk Assessment," February, 2022. (U).

Exhibit 201: (U) Website of Etherscan, "Block #1400000," [redacted] available at: https://etherscan.io/block/11400000. (U).

Exhibit 202: (U) Website of Department of the Treasury, Press Releases, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," August 8, 2022. Available at: https://home.treasury.gov/news/press-releases/jy0916 (U).

Exhibit 203: (U) Website of Investopedia, "What is Decentralized Finance (DeFI) and How Does It Work? [redacted] available at: investopedia.com/decentralized-finance-defi-5113835. (U).

Exhibit 204: (U) Website of The Block.co, "Tornado Cash DAO votes to Take Partial Control Over Treasury Funds," August 12, 2022, [redacted] available at: theblock.co/post/163274/tornado-cash-dao-votes-to-take-partial-control-over-treasury-funds. (U).

Exhibit 205: (U) Website of the Department of the Treasury, Financial Sanctions, "Frequency Asked Questions #562," March 19, 2018, available at: https://home.treasury.gov/policy-issues/financial-sanctions/faqs/562. (U).

Exhibit 206: (U) Website of Github, "Tornado Cash Core," available at: https://github.com/tornadocash/tornado-core. (U).

Exhibit 207: (U//~~FOUO~~) Memorandum for Record, "Blockchain Analysis of Heists Using Tornado Cash," October 13, 2022. (U//~~FOUO~~).

Exhibit 208: (U) Website of Github, "Roman Semenov," [redacted] available at: https://github.com/poma?tab=overview&from=2019-11-01&to=2019-11-30. (U).

Exhibit 209: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 1, [redacted] available at: https://github.com/tornadocash/tornado-core/commits/master?before=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+35&branch=master&qualified_%E2%80%A6. (U).

Exhibit 210: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 2, [redacted] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+34&branch=master&qualified_na%E2%80%A6. (U).

Exhibit 211: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 3, [redacted] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+69&branch=master&qualified_na%E2%80%A6. (U).

Exhibit 212: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 4, [redacted] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+104&branch=master&qualified_n%E2%80%A6. (U).

Exhibit 213: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 5, [redacted] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+139&branch=master&qualified_n%E2%80%A6. (U).

Exhibit 214: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 6, [redacted] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+174&branch=master&qualified_n%E2%80%A6. (U).

Exhibit 215: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 7, [redacted] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+209&branch=master&qualified_n%E2%80%A6. (U).

Exhibit 216: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 8, [redacted] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+244&branch=master&qualified_n%E2%80%A6. (U).

Exhibit 217: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 9, [redacted] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+279&branch=master&qualified_n%E2%80%A6. (U).

Exhibit 218: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 10, [redacted] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+314&branch=master&qualified_n%E2%80%A6. (U).

Exhibit 219: (U) Website of General Services Administration, Digital.gov, "An introduction to GitHub," [redacted] available at: https://www.theregister.com/Profile/about_the_register/. (U).

Exhibit 220: (U) Website of CoinDesk, "What Are Liquidity Pools?" June 7, 2022, accessed October 24, 2022, available at: https://www.coindesk.com/learn/what-are-liquidity-pools/. (U).

Exhibit 221: (U) Website of Ethereum, "What is Staking?" [redacted] available at: https://ethereum.org/en/staking/ (U).

Exhibit 222*: (U) Website of NIST, "Glossary, Publishing Node," accessed October 24, 2022https://csrc.nist.gov/glossary/term/publithis dushing_node#:~:text=Definition(s)%3A,%2C committing node%2C minting node.

Exhibit 223: (U) Website of PCMagazine, "Encyclopedia, Off-Chain Governance," accessed October 24, 2022, available at: https://www.pcmag.com/encyclopedia/term/off-chain-governance#:~:text=Modifications to a blockchain that, is how a DAO operates. (U).

Exhibit 224: (U) Website of PCMagazine, "About, " accessed October 25, 2022, available at: https://www.pcmag.com/about. (U).

Exhibit 225: (U) Website of Elliptic, "the $100 Million Horizon Hack: Following the Trail Through Tornado Cash to North Korea," July 13, 2022, available at: hub.elliptic.co/analysis/the-100-million-horizon-hack-following-the-trail-through-tornado-cash-to-north-korea/. (U).

Exhibit 226: (U) Website of Gemini, "Crypto Wallets, Custodial vs Non-Custodial," updated May 6, 2021 [redacted] vailable at: https://www.gemini.com/cryptopedia/crypto-wallets-custodial-vs-noncustodial/ (U).

Exhibit 227: (U) Website of Gemini, "About," [redacted] available at: https://www.gemini.com/about. (U).

Exhibit 228: (U) Website of PCMagazine, "Encyclopedia, pseudo-random," accessed November 1, 2022, available at: https://www.pcmag.com/encyclopedia/term/pseudo-random-numbers. (U).

Exhibit 229: (U) Website of GitHub, "Creating a Repository," [redacted] available at: https://docs.github.com/en/get-started/quickstart/hello-world. (U).

EXHIBIT 4

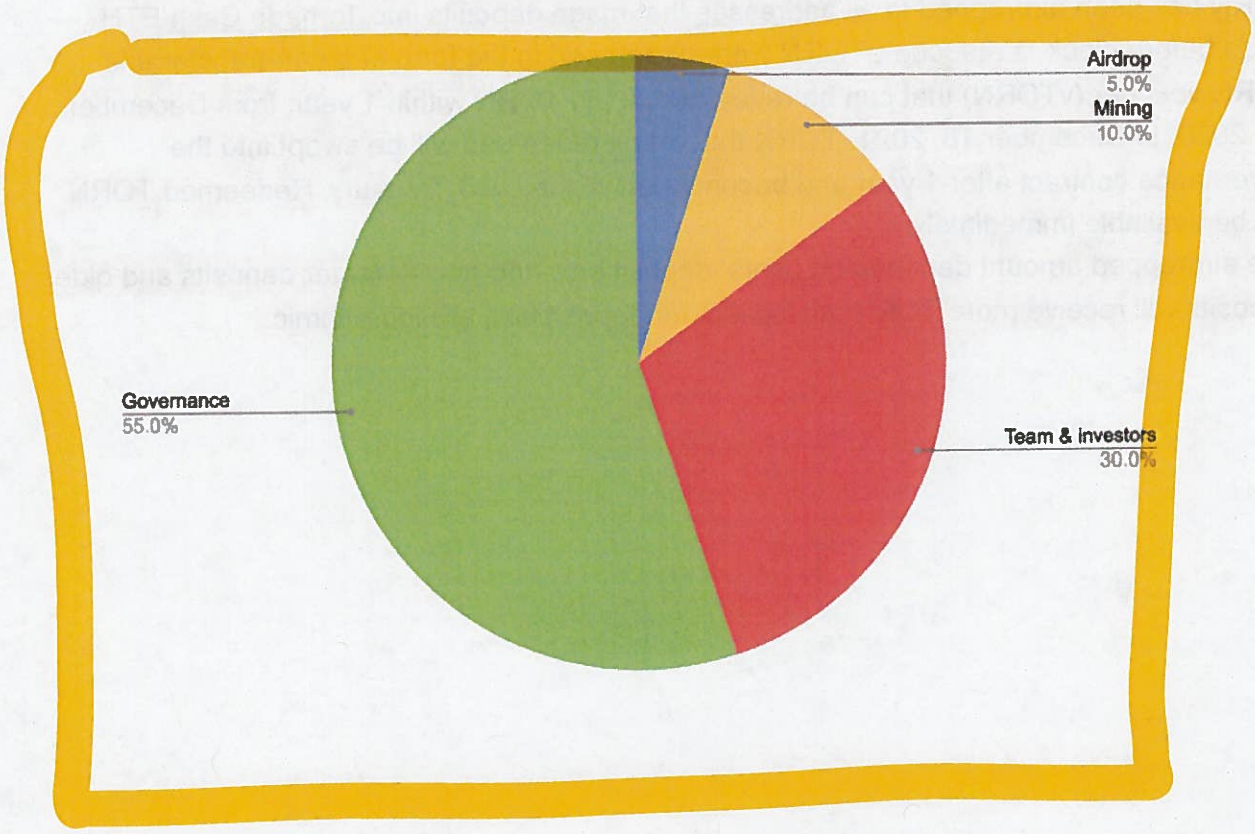
TORN - tornado.cash

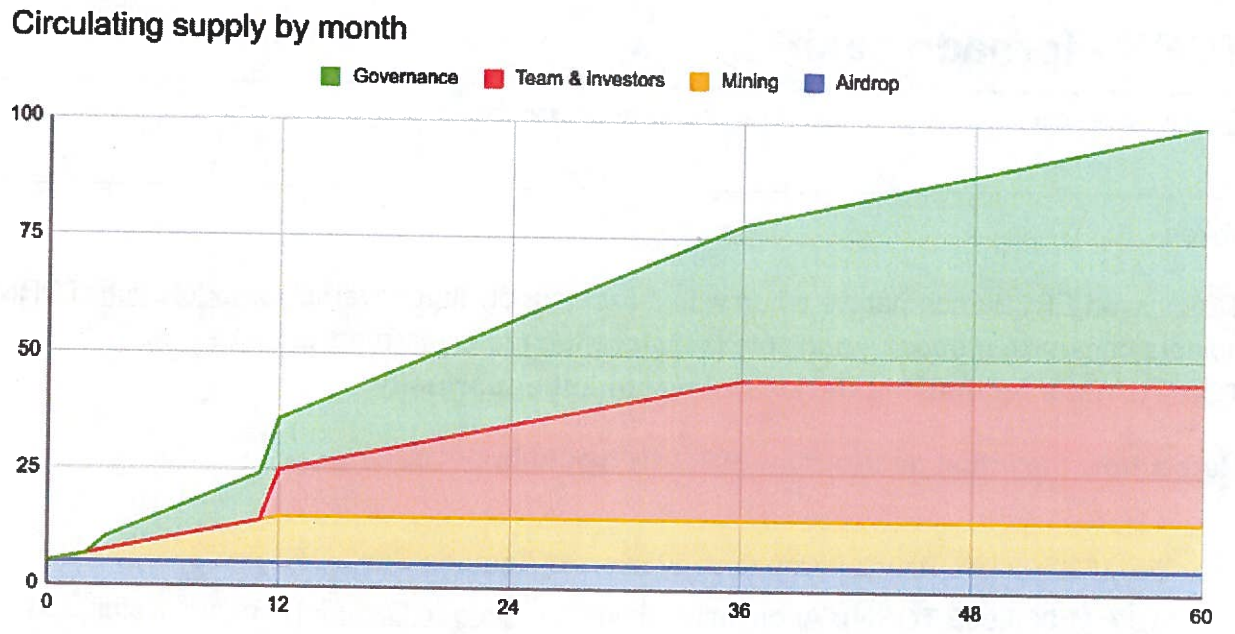
Token

TORN is an ERC20-compatible token with a fixed supply that governs Tornado.Cash. TORN holders can make proposals and vote to change the protocol via governance.
TORN is not a fundraising device or investment opportunity.

Here's how the initial distribution of TORN would break down:

5% (500,000 TORN): Airdrop to early users of Tornado.Cash ETH pools
10% (1,000,000 TORN): Anonymity mining for Tornado.Cash ETH pools, distributed linearly over 1 year
55% (5,500,000 TORN): DAO treasury, will be unlocked linearly over 5 years with 3 month cliff
30% (3,000,000 TORN): Founding developers and early supporters, will be unlocked linearly over 3 years with 1 year cliff





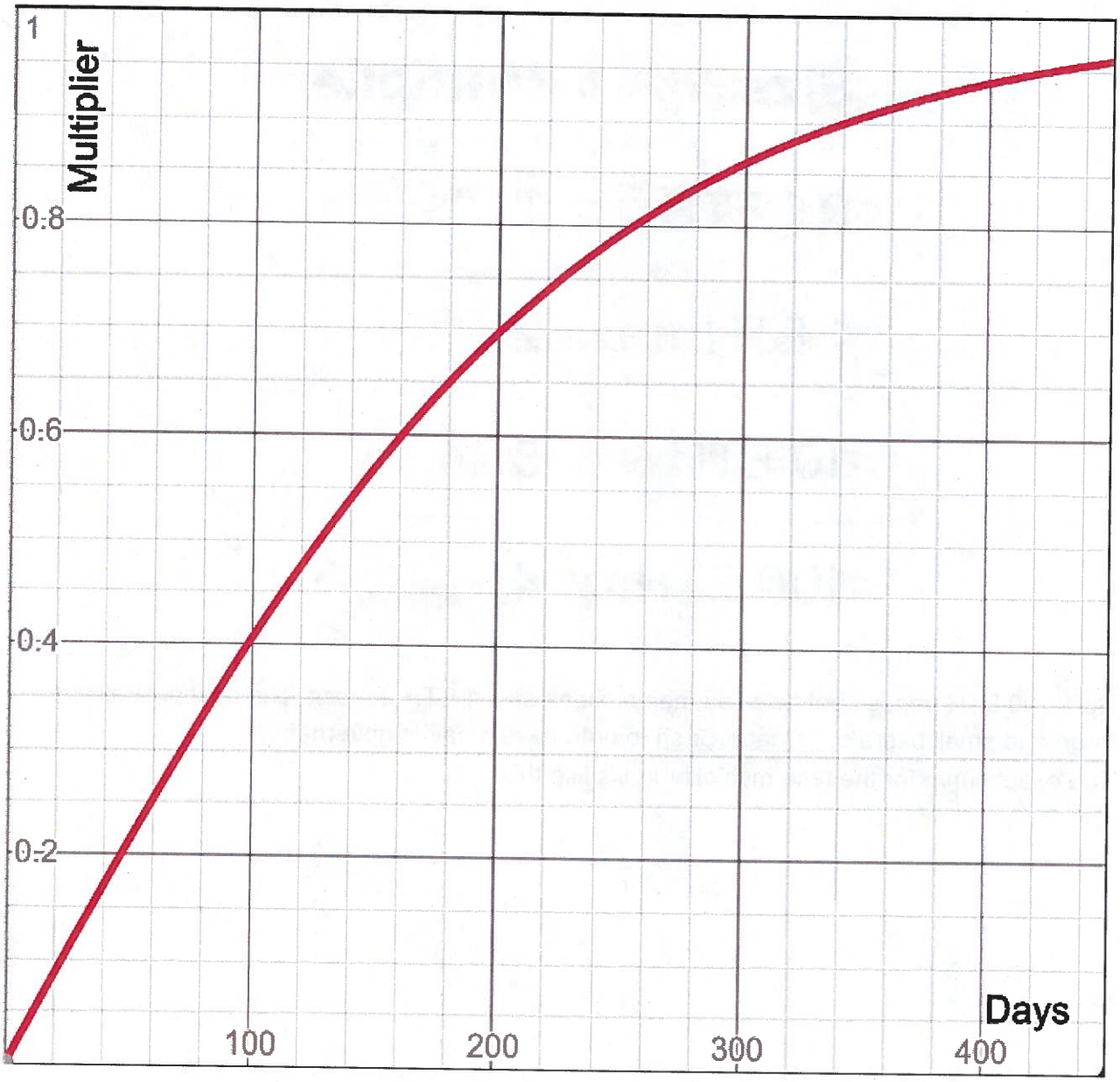
Airdrop

Users who have believed in Tornado.Cash from early on should have a say in governing the protocol. For this reason, early adopters of the protocol did receive an airdrop of TORN. TORN has been airdropped to all addresses that made deposits into Tornado.Cash ETH pools before block `11400000`. TORN were airdropped in the form of a non-transferable TORN voucher (vTORN) that can be redeemed 1:1 to TORN within 1 year, from December 18, 2020, to December 18, 2021. TORN that aren't redeemed will be swept into the governance contract after 1 year and become part of the DAO Treasury. Redeemed TORN will be available immediately.

The airdropped amount depends on users' deposit size and age — larger deposits and older deposits will receive more TORN. Multipliers for deposit size are logarithmic:

Size	Multiplier
0.1 ETH	1
1 ETH	2
10 ETH	3
100 ETH	4

So a 100 ETH deposit get twice as many tokens as a 1 ETH deposit. The multiplier allows large and small users of Tornado.Cash to both have a say in governance.
The exact curve for the time multiplier looks like this:



The exact airdrop formula is the following:

$$TORN = W * (\log(amount) + 2) * (\frac{2}{1 + e^{-k*blocks}} - 1)$$

$$k = 0.0000015$$

$$W = 25.3$$

Written by ***Tornado Team***

EXHIBIT 22

CHRISTIAAN VOS

JUL 14, 2022

What is a crypto airdrop, and how does it work?

Crypto airdrops are a marketing strategy used by startups to give tokens to existing cryptocurrency traders for free or in exchange for minimal promotional work.

3367 70

7:36

Almost daily there are new crypto airdrops, with some easier to obtain than others. Not every airdrop is equally reliable. Crypto airdrops always seem very lucrative at first, but they can also cause problems. To make sure you can profit from crypto airdrops but also see through any pitfalls, you can read all about crypto airdrops and how they work in this article!

What is a crypto airdrop?

A crypto airdrop is a method by which you can earn free crypto from a crypto project. There are several ways to receive these tokens. Many times an airdrop is associated with free cryptocurrencies, but this is not necessarily true. You have to put in time and effort or you may have to deal with transaction fees. However, it is also possible to participate in an airdrop for free!

Related: What is cryptocurrency? A beginner's guide to digital currency

You're probably wondering; how do crypto airdrops work? Crypto projects have a certain amount of available tokens that they give to people who meet eligibility requirements. By completing tasks, you can become eligible for these tokens. There are several ways to participate in crypto airdrops. Often you have to sign up for an airdrop or perform other actions. After completing tasks or winning the tokens, you can claim them or they will be deposited into your wallet.

Examples of crypto airdrops

There have been hundreds of airdrops in the past, including the airdrops of leading crypto projects. There are therefore a huge number of examples of crypto airdrops. Airdrops have been occurring for years in the crypto world. The first airdrop ever took place back in 2014. Back then, a crypto project even handed out 50% of all tokens during an airdrop.

The crypto project, called Auroracoin, has its cryptocurrency token, known as AUR. The project had plans to make AUR the national cryptocurrency of Iceland. Therefore, the entire AUR airdrop went to Icelandic citizens, who could receive a total of 31 AUR per individual.

Many airdrops also followed in the years after the Auroracoin airdrop, including those of slightly more well-known cryptocurrencies. For example, in 2016 and 2017, respectively, Stellar Lumens (XLM) and Bitcoin Cash (BCH) organized cryptocurrency airdrops, distributing their airdrop coins to Bitcoin owners. Bitcoin Cash gave away one Bitcoin Cash token per Bitcoin, which was worth thousands of dollars at its peak.

Another well-known crypto airdrop is UniSwap's airdrop, in which the governance token UNI was given out to users of the decentralized exchange (DEX) in 2020. In total, over 250,000 accounts received 400 UNI per account, which totals thousands of dollars per person! A very lucrative airdrop if you can sell your UNI tokens at the right time.

Different types of crypto airdrops

There are several different types of airdrops all of which have unique characteristics. Crypto projects often see airdrops as a marketing tool where they try to grow as a project through the airdrop. For example, projects may be looking for more brand awareness and new users or they may want to reward their first users.

The motive of a crypto project is of course related to the type of airdrop. There are a few types of crypto airdrops that are common, namely:

Standard airdrop

In a standard airdrop, tokens are distributed for free and you do not have to perform any particular actions. All you have to do i create an account somewhere and then give your wallet address. There may be only a certain amount of tokens available for th airdrop, so you need to get there early.

These crypto airdrops are hugely popular because you can participate easily and it is free crypto because of this. To distribute

the tokens fairly, the distribution can take place via a draw. In this case, you have a chance to win free crypto, but you are not guaranteed to win the airdrop.

Bounty airdrop

With bounty airdrops, you can receive rewards for completing tasks. These tasks take a fair amount of work, so the price you pa for free cryptocurrency tokens consists of energy and effort. Often the tasks are not difficult but are valuable for a crypto proje This is why new projects are increasingly choosing this method of token airdrops. Some examples of the activities are:

Examples of activities for which bounty airdrops are awarded

Holder airdrop

With a holder airdrop, you can receive cryptocurrency tokens if you hold a certain number of tokens of another cryptocurrency. The amount of your airdrop is determined based on a snapshot. At a certain moment, a snapshot of your crypto wallet is made. This moment is often a fixed date, but it can also be during a certain period. Based on the amount of tokens in your wallet, you can expect to receive a certain amount of cryptocurrencies.

How can you find upcoming crypto airdrops?

You can find upcoming crypto airdrops in several ways. Of course, you can consult search engines like Google, and several websites have mapped out the current airdrop offerings. Often you can find not only airdrops in progress, but also upcoming airdrops.

Some websites do not show questionable airdrops in advance because they do not want to risk their reputation. Some platform indicate the extent to which they trust the airdrop in question. Regardless of the opinion of an airdrop website, it is still wise to do your research and pay close attention to an airdrop.

In addition, there are often crypto platforms that launch airdrops for people who have used the platform in the past. These people then become eligible, without knowing it beforehand. To qualify for possible airdrops, you can start using swap platforms. When you use swap platforms that are built on a blockchain with low transaction fees, you can qualify for an airdrop very cheaply.

How do NFT airdrops work?

Most airdrops are about cryptocurrencies, but there are also airdrops where you can get nonfungible tokens (NFTs). Just like crypto airdrops, NFT airdrops can be organized for promotional purposes. If you want to qualify for an NFT airdrop, there are several ways to accomplish this.

Related: How to store NFT assets — A beginner's guide

Sometimes you have to perform certain tasks, just like with the crypto airdrops, but the token issue can also be done through a lottery. In addition, you may also need to own another nonfungible token from a particular NFT collection to qualify for the airdrop. For example, owners of a Bored Ape Yacht Club (BAYC) NFT received ApeCoin tokens as airdrops. NFT airdrops can also involve risks, as airdrop phishing also occurs at NFTs. Therefore, always make sure that you only participate in reliable airdrops and never share your data.

Are crypto airdrops safe?

Often crypto airdrops seem harmless and safe, but this is not always the case. Scammers have also found ways to scam people through airdrops. They have found ways to harm crypto enthusiasts by taking away cryptocurrencies or private keys.

Stay alert and pay close attention to airdrops, especially when high amounts are promised that are too good to be true. It is important to remember that it is never wise to connect your crypto wallet to an untrustworthy party or give up your private keys.

There have even been fraudulent airdrop actions where scammers deposited cryptocurrencies. These tokens turned out to be fake and were unsaleable. To make sure you don't become a victim of a scam, it can be useful to research the team behind the crypto project and find out what others think.

Subscribe

By subscribing, you agree to our
Terms of Services and Privacy Policy

#Blockchain #Cryptocurrencies #Ethereum #Technology #Fintech #Tokens #Airdrop #DeFi #NFT #How to Crypto

RELATED NEWS

How to get a job in the Metaverse and Web3

Boxing champion throws his weight behind NFTs that aim to raise funds for Ukraine

What is Sorare, and how to play it?

Indian government's 'blockchain not crypto' stance highlights lack of understanding

How to convert your digital art into NFTs and sell it

How to get premium high-resolution metaverse and NFT images

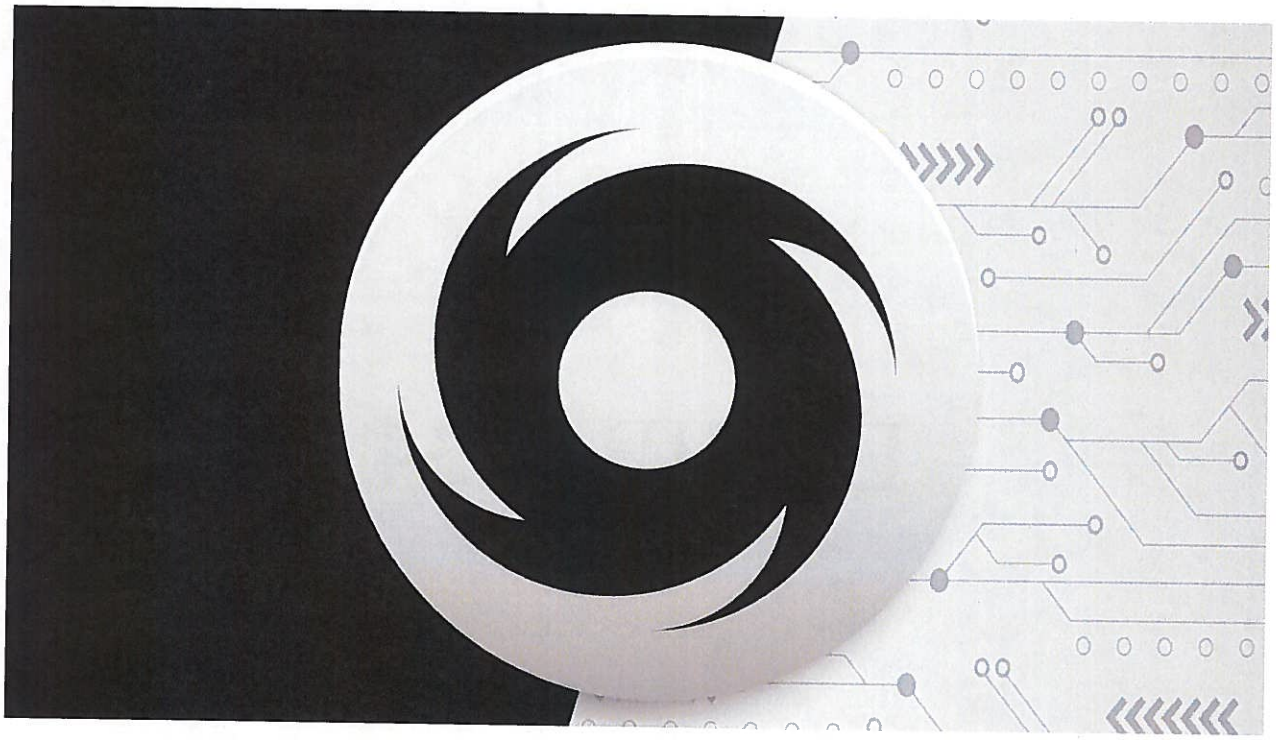
Load More Articles

EXHIBIT 34

Tornado Cash Governance Token TORN Shudders More Than 57% Since the US Government Ban

news.bitcoin.com/tornado-cash-governance-token-torn-shudders-more-than-57-since-the-us-government-ban/

August 13, 2022



Amid the crackdown against Tornado Cash, associated addresses, contributing developers, and anyone who uses the mixing platform, the project's governance token called TORN has shuddered in value. TORN is an ERC20 with a fixed supply that is leveraged for governance proposals and voting. During the last seven days, the Tornado Cash governance token has lost 57.6% in value against the U.S. dollar.

Tornado Cash Token Loses More Than Half of Its Value This Week

It seems that everything Tornado Cash touched is tainted and during the last week, the project's governance token tornado cash (TORN) has lost more than half of its USD value. TORN is an ERC20-based token that was launched in February 2021, and 5% of the supply was airdropped to users who had leveraged the mixing application before the snapshot.

There's approximately 1,511,065 TORN tokens and 500,000 TORN was airdropped to the Tornado Cash community. Since the U.S. government cracked down on Tornado Cash and banned the mixing application alongside associated ETH-based addresses, TORN has taken a severe market beating.

TORN has seen $43.4 million in global trade volume and a lot of it stems from selling. Popular crypto exchanges that list TORN include Binance, Bingx, and Bitget. 69.93% of all TORN trades today are paired against USDT, which is followed by BUSD (24.73%), BTC (3.92%), WETH (1.18%), and USDC (0.24%).

Additionally, 30% of the TORN stash was reserved for devs and contributors, and vested for a three-year linear vesting period with a one-year cliff. TORN is down 97.2% from the crypto asset's all-time high on February 13, 2021.

TORN tapped an all-time low hours ago on Saturday morning (EST) hitting 11.81 per unit on August 13. If the TORN market rout continues, vested stashes of the ERC20 will be worth less and less as time passes. The U.S. government's sanctions against the mixer Tornado Cash may cause TORN investors to continue dumping after losing faith in the project.

Tags in this story

57% down, Binance, Bingx, Bitget, crypto assets, ERC20, ERC20-based token, ETH mixing service, ETH token, Exchange, governance coin, Markets, pairs, Token, TORN, TORN governance, TORN holders, Tornado cash, tornado cash coin, trading, USDT Pair, Voting

What do you think about the tornado cash (TORN) coin losing significant value this past week? Let us know what you think about this subject in the comments section below.

Jamie Redman

Jamie Redman is the News Lead at Bitcoin.com News and a financial tech journalist living in Florida. Redman has been an active member of the cryptocurrency community since 2011. He has a passion for Bitcoin, open-source code, and decentralized applications. Since September 2015, Redman has written more than 5,700 articles for Bitcoin.com News about the disruptive protocols emerging today.

***Image Credits**: Shutterstock, Pixabay, Wiki Commons*

Previous article

Axie Infinity Surpasses $4 Billion in All-Time Sales, Team Removes SLP Rewards From Classic Game Mode

Next article

Crypto Trading, Investing Illegal in Iran, Central Bank Governor Reiterates

Read disclaimer

Show comments

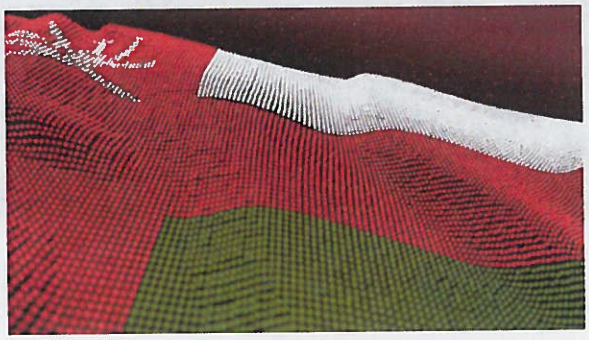
More Popular News

In Case You Missed It

Today's Top Ethereum and Bitcoin Mining Devices Continue to Rake in Profits

As the crypto economy hovers just under $2 trillion in value, application-specific integrated circuit (ASIC) mining devices are making decent profits. While ASIC miners can still mine ethereum, a 1.5 gigahash (GH/s) Ethash mining device can rake in $51.58 per ... read more.

In Case You Missed It

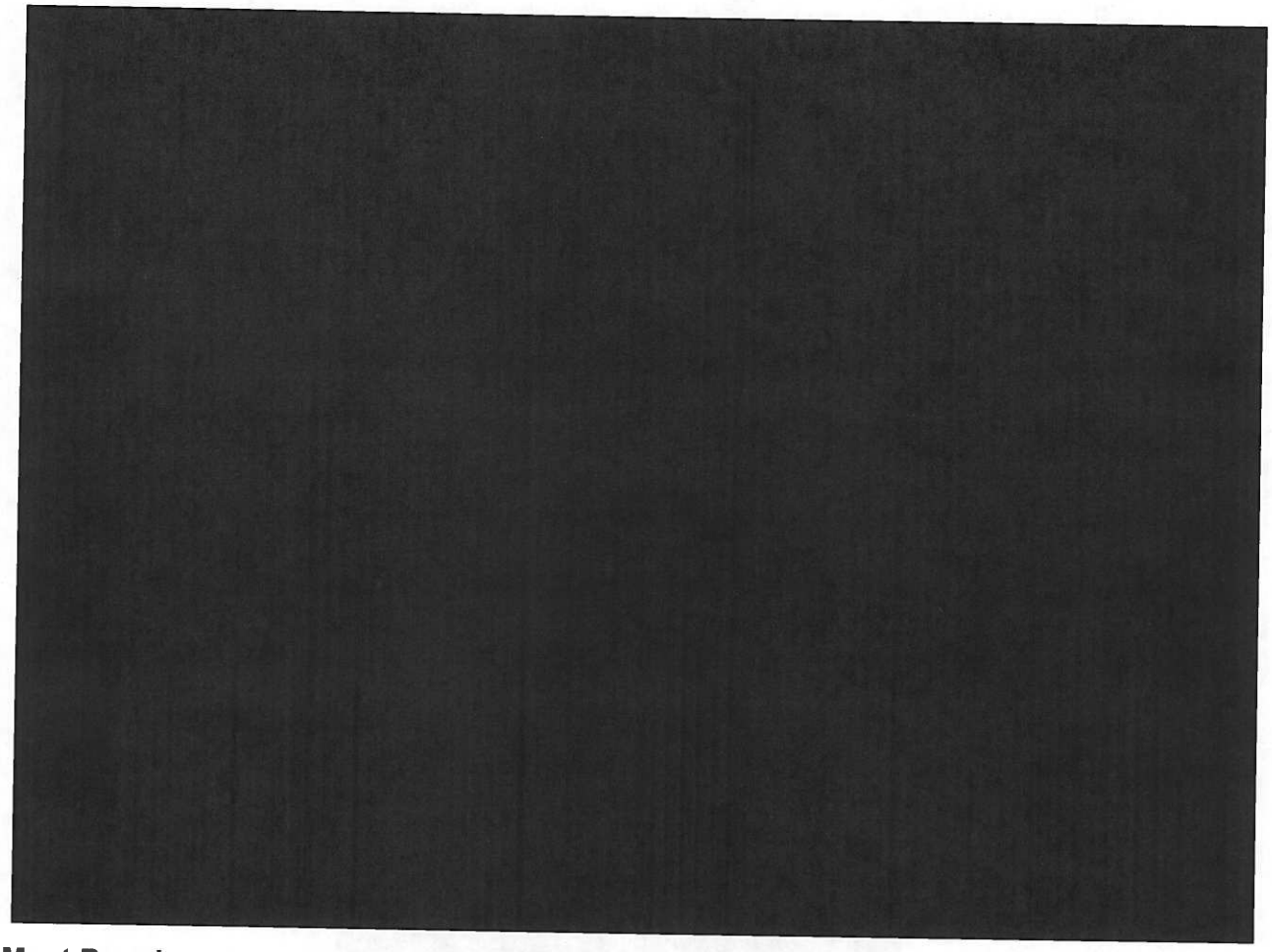


Oman to Incorporate Real Estate Tokenization in Virtual Assets Regulatory Framework

Real estate tokenization is set to be incorporated into Oman Capital Markets Authority (OCMA)'s virtual asset regulatory framework. According to an advisor with the authority, the tokenizing of real estate will open investment opportunities for local and foreign investors. Real ... read more.

The Latest

[redacted]



Most Popular

Press releases

Check all the news here

NEWS

EXHIBIT 39

Tornado.cash Trusted Setup Ceremony

tornado-cash.medium.com/tornado-cash-trusted-setup-ceremony-b846e1e00be1

Tornado Cash May 4, 2020

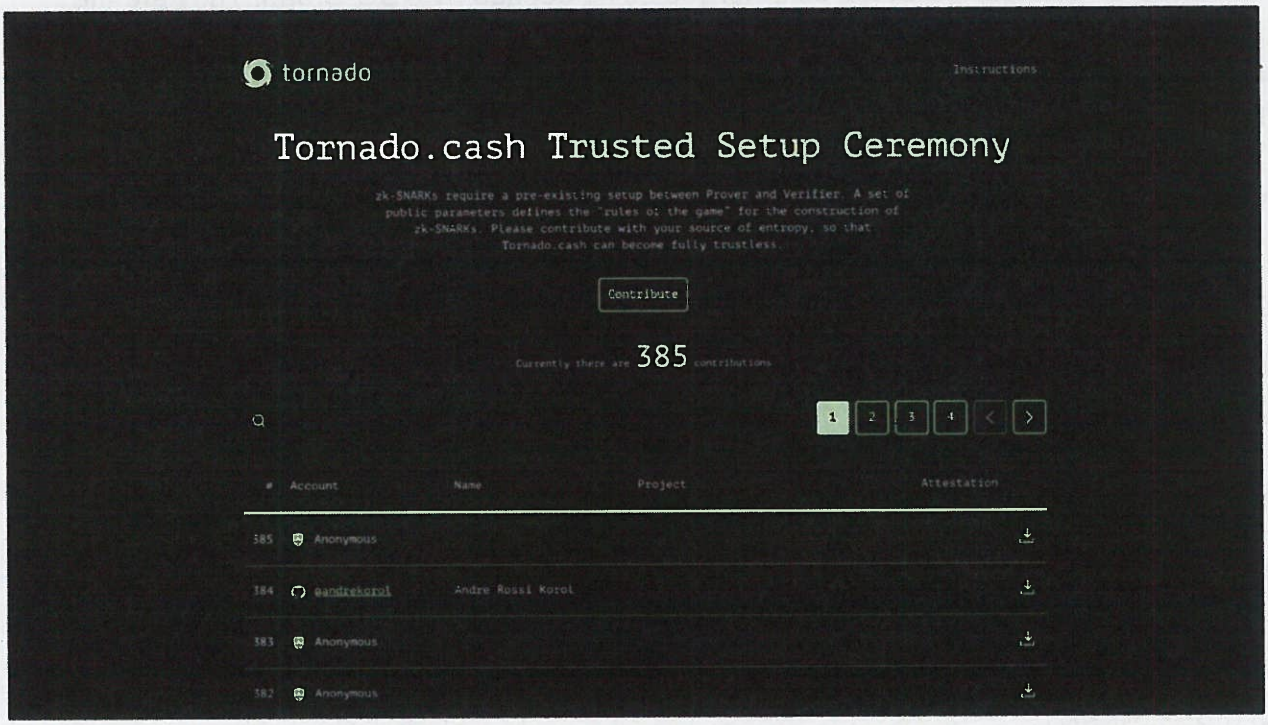
Tornado Cash

May 1, 2020

·

3 min read

We are happy to announce that Tornado.cash trusted setup ceremony has been launched. We ask crypto community to help make Tornado.cash fully trustless by contributing to the ceremony.



What does it mean?

Tornado.cash utilizes zk-SNARK technology to provide anonymity for withdrawals. The zk-SNARK requires a trusted setup which is a special procedure that generates the prover and verifier keys. In order to make sure that it is done in a secure way, no one is be able to fake proofs or steal user funds it should be done in a decentralized way. To fake zk proofs, an

attacker must compromise every single participant of the ceremony. Therefore, the probability of it goes down as the number of participants goes up. The purpose of the ceremony is to generate Verifier smart contract. After completion, our team will update all Verifiers in all instances and set the operator address to zero. At this point Tornado.cash smart contracts will become completely immutable and unstoppable.

How do I participate?

Simply open ceremony.tornado.cash and click on the Contribute button.
You can choose to make your contribution anonymously or Sign In with your github/twitter account to have your identity linked to it. If you would like to be part of the ceremony in the forever immutable smart contract, please contribute with your source of entropy.

If you are an advanced user you can contribute more securely by using these instructions and compiling the source code yourself. It should be fairly easy!

Security audit

The code for our Trusted Setup ceremony is being audited by NCC Group. They are the same group of folks that audited the ZCash ceremony and it is being sponsored by Moloch DAO. The audit report will be released shortly and will show that we fixed all important issues.

Why is it called Phase 2?

Trusted setup for Groth16 SNARKS is done in 2 steps. The first step is universal for all SNARKs and is called Powers of Tau. The second step is called Phase 2 and is circuit-specific, so it should be done separately for each different SNARK. Our phase 2 is based on 30th contribution to Perpetual Powers of Tau ceremony.

Is it open source?

Of course! You can find the ceremony code here and the UI source code here.

Are my private notes affected?

No! You will still keep all your deposits. The changes will only affect Verifier smart contract. The rest of the smart contracts and their state will not be changed. However, the safety and security of your deposits will automatically increase after the ceremony is finished.

When will it be finalized?

We plan to end the ceremony on May 10th 2020. If there is high demand, we will keep it open for a couple more days.

Potential UX issues

Due to the nature of MPC (multi-party computation), it behaves like mining in PoW systems. In essence, the UI has to download the latest contribution and compute your new hash based on the previous one. If someone has already submitted a new contribution during your computation, you will no longer have the latest one and the process will need to restart. Therefore, since the page expects possible failures it will try to make 3 additional attempts. This might require for you to stay on the page for a little while. Please be patient. In a rare instance, when all of the attempts were unsuccessful, please refresh the page and try again.

Acknowledgments

We'd like to thank Koh Wei Jie, Kobi Gurkan, and BarryWhiteHat for building Perpetual Powers of Tau ceremony and Moloch DAO for funding NCC group security audit of the ceremony code. Lastly, we would like to thank the entire Ethereum community for supporting us and contributing to our Gitcoin grant.

EXHIBIT 48

tornado-repositories

Overview | Repositories 34 | Projects | Packages | People

README.md

Tornado-Repositories: an archival fork of the Tornado Cash source code

These repositories contain an archival fork of the Tornado Cash and Tornado Cash Nova source code base. They are maintained on Github by Matthew D. Green of Johns Hopkins for teaching and research purposes.

See also: EFF blog post.

What is Tornado Cash and what is this repository?

Tornado Cash and Tornado Nova are open-source coin mixing tools that were developed by an independent team of software developers and deployed onto Ethereum and several other blockchains. On August 8, 2022 the Office of Foreign Assets Control (OFAC), a division of the US Treasury, declared "Tornado Cash" and "Tornado Cash Nova" to be Specially Designated Nationals (SDNs): the result was to effectively sanction the Tornado Cash organization, its software development repositories, and the main smart contract deployment on Ethereum.

This move to sanction Tornado Cash represents the first instance in which the US government has applied economic sanctions to an open source software project. As a result of this announcement, several cryptocurrency exchanges have banned users who interact with the Tornado Cash smart contract address on Ethereum. Within hours of the OFAC announcement, Github shut down the user accounts of all known Tornado Cash developers and removed the source code repositories owned by Tornado's Github organization.

While Github succeeded in removing the original copies of all Tornado source code repositories, they did not remove all "forks" of the code made by GitHub users. Several of these forks were recently collected and (further) forked by contributors to the tornadocash-community organization. Those folks did the hard work. The current repository is simply another fork of the repositories they collected. (Note: some additional repositories have since been added, see below.)

Why preserve the Tornado Cash source code?

In my work as a researcher and instructor at Johns Hopkins, I've made extensive use of the Tornado Cash and Tornado Nova source code to teach concepts related to cryptocurrency privacy and zero-knowledge technology. My students have built amazing projects from the code. The loss or decreased availability of this source code will be harmful to the scientific and technical communities.

Moreover, I am uncomfortable with the implications of the Github decision. Github is a private company, and of course it can suspend users for any perceived violation of its Terms of Service. At the same time, it is hard to believe that Github's decision was unrelated to the government's action. In my opinion it is much more likely that Github censored the Tornado Cash code repositories as part of a risk-mitigation procedure they engaged in *as a direct result of the OFAC order*. More critically: I believe that this removal of protected speech was a predictable consequence of OFAC's action, one that Treasury could easily have forseen and taken steps to avoid.

Given that much of the Internet publishing infrastructure is operated by private firms, the Tornado Cash example raises the prospect that the US government may use sanctions to ban source code distribution and scientific speech. Because sanctions rules are broad and carry extreme penalities, these speech bans do not need to be accomplished through explicit orders: they can be obtained simply by exposing US companies and citizens to the perception of sanctions risk. The result is a "chilling effect" on speech, one that allows the US government to determine which citizens and organizations do or do not enjoy the right to publish their source code and scientific artifacts.

The creation of this archival repository organization does not solve this issue. Nor will it repair the damage that has already been done by the OFAC order. The purpose of this repository is to make it clear to the US Treasury Department and Github that *this code has value*, and its removal has consequences that affect scientific researchers and students in the United States. Moreover, it exists to test the proposition that code removal should ever been an appropriate future response to a sanctions order, no matter how justified the order itself may be. I have discussed my concerns with the Electronic Frontier Foundation and they have agreed to represent me as a client. See their blog post here.

Why are you hosting this on GitHub...? Can't GitHub just take down this organization?

GitHub, as one of the most widely-used software distribution websites in the world, is an ideal place to host this repository. Deploying software on GitHub is more reliable than self-hosting on servers at the University: because of this I routinely use GitHub to host course material for my classes. At this moment I have no reason to believe that GitHub is opposed to the hosting of Tornado Cash's source code for non-deployment purposes.

GitHub may see things differently: if so, that would be fascinating. It goes without saying that I have made offline copies of all these repositories and will immediately re-publish them in a different location (such as a University server) if this site becomes inaccessible.

But Git is decentralized (and IPFS exists) so why do we care about GitHub?

Git is a decentralized version control system. Hence other copies of the Tornado Cash code certainly exist on other machines and at other locations (in fact, go ahead and make a clone right now!) You should be able to verify that these are authentic by comparing hashes to a main trusted repository, like the one that used to be hosted here on Github. (Since that no longer exists, you can use the forks in this repository. Alternatively here's a Wayback Machine copy that still sort of works.)

Hence Github's removal of the Tornado Cash code repositories and developer accounts is not a total ban on the source code. It does have two critical effects: first, it halts the ongoing development of this source code *even as a pure software development and research project.* Second, it makes discovery of the code much more difficult. (It is more analogous to removing a book from major commercial bookstores, while still allowing users to exchange PDF files on USB sticks.) At present a non-expert user searching Google to find the Tornado Cash source will have a difficult time. Try it yourself!

If you want a copy of the code on a more durable decentralized medium, there are copies of (limited) repositories on IPFS. I certainly don't warranty these (or any of this code), and you should carefully check hashes against the repositories on Github and in the Wayback Machine just in case:

- Tornado Nova: `ipfs://bafybeiho72nozeq2mi6egptem77omhujt5ovpx4jjskg5sz2ti57zlunmm`
- Tornado Cash Classic:
  `ipfs://bafybeicu2anhh7cxbeeakzqjfy3pisok2nakyiemm3jxd66ng35ib6y5ri`

You can also find recent clones of the Tornado Cash repositories on Software Heritage.

Will you take PRs for Tornado Cash, or host other projects?

These repositories are intended as an archival project only. They are yours to clone and fork. They will not be actively developed, which means that over time they will gradually become obsolete. If open source Tornado Cash development resumes (even under a different team of developers), I may periodically clone copies of their repositories here. In the future this organization may also evolve to host archival forks of other non-TC privacy projects, should I determine that they are also at risk of sanctions-based code removal.

Additional repositories

After adding the initial repositories, several additional repositories were provided by anonymous contributors. These will be added one at a time after I have a chance to manually verify the hashes against cached copies of the original GitHub website. So far the public repositories include:

- tornado-onion
- tornado-trees-proposal

A new repository called GOOGLE_CACHE contains details on the hash verification, as well as links/copies of the cached web pages.

Popular repositories

tornado-core — Public
Forked from tornadocash-community/tornado-core
JavaScript ☆ 64 46

tornado-verified-forks — Public
Forked from tornadocash-community/tornado-verified-forks
List of verified forks from tornadocash official repos
☆ 18 13

tornado-nova — Public
Forked from tornadocash-community/tornado-nova
Tornado-nova fork
Solidity ☆ 8 18

tornado-classic-ui — Public
Forked from tornadocash-community/tornado-classic-ui
JavaScript ☆ 8 16

.github — Public
☆ 8 2

deployer — Public
Forked from tornadocash-community/deployer
JavaScript ☆ 5 10

[redacted]

Repositories

Find a repository...

Type Language Sort

tornado-core Public
JavaScript 64 GPL-3.0 77 0 1 Updated 5 days ago

.github Public
8 2 0 0 Updated 10 days ago

GOOGLE_CACHE Public
HTML 0 0 0 0 Updated 10 days ago

tornado-classic-ui Public
JavaScript 8 MIT 40 0 1 Updated 13 days ago

tornado-relayer Public
JavaScript 1 13 0 1 Updated 15 days ago

tornado-trees-proposal Public
JavaScript 0 MIT 0 0 0 Updated 19 days ago

tornado-onion Public
0 0 1 0 Updated 19 days ago

deployer Public
JavaScript 5 MIT 17 0 0 Updated on Aug 10

tornado-root-updater Public
JavaScript 2 MIT 15 0 0 Updated on Aug 10

tornado-verified-forks Public
List of verified forks from tornadocash official repos

18 MIT 36 0 0 Updated on Aug 10

View all repositories

People

This organization has no public members. You must be a member to see who's a part of this organization.

Top languages

JavaScript TypeScript HTML Solidity Shell

EXHIBIT 54

U.S. DEPARTMENT OF THE TREASURY

Treasury Takes Robust Actions to Counter Ransomware

September 21, 2021

Targets First Virtual Currency Exchange for Laundering Cyber Ransoms

OFAC Updates Ransomware Advisory to Encourage Reporting and Cyber Resilience

WASHINGTON — As part of the whole-of-government effort to counter ransomware, the U.S. Department of the Treasury today announced a set of actions focused on disrupting criminal networks and virtual currency exchanges responsible for laundering ransoms, encouraging improved cyber security across the private sector, and increasing incident and ransomware payment reporting to U.S. government agencies, including both Treasury and law enforcement. Treasury's actions today advance the United States government's broader counter-ransomware strategy, which emphasizes the need for a collaborative approach to counter ransomware attacks, including partnership between the public and private sector and close relationships with international partners.

"Ransomware and cyber-attacks are victimizing businesses large and small across America and are a direct threat to our economy. We will continue to crack down on malicious actors," said Treasury Secretary Janet L. Yellen. "As cyber criminals use increasingly sophisticated methods and technology, we are committed to using the full range of measures, to include sanctions and regulatory tools, to disrupt, deter, and prevent ransomware attacks."

Ransomware attacks are increasing in scale, sophistication, and frequency, victimizing governments, individuals, and private companies around the world. In 2020, ransomware payments reached over $400 million, more than four times their level in 2019. The U.S. government estimates that these payments represent just a fraction of the economic harm caused by cyber-attacks, but they underscore the objectives of those who seek to weaponize technology for personal gain: to disrupt our economy and damage the companies, families, and individuals who depend on it for their livelihoods, savings, and futures. In addition to the

millions of dollars paid in ransoms and recovery, the disruption to critical sectors, including financial services, healthcare, and energy, as well as the exposure of confidential information, can cause severe damage.

Some virtual currency exchanges are a critical element of this ecosystem, as virtual currency is the principal means of facilitating ransomware payments and associated money laundering activities. The United States has been a leader in applying its anti-money laundering/countering the financing of terrorism (AML/CFT) framework in the virtual currency area, including with the Financial Crimes Enforcement Network (FinCEN) publishing guidance regarding the application of Bank Secrecy Act rules in this area in 2013 and 2019. FinCEN has also taken important enforcement action against non-compliant virtual currency money transmitters facilitating ransomware payments, such as BTC-e in 2017 and the virtual currency mixing service Helix in 2020. In addition, the United States is taking steps to improve transparency regarding ransomware attacks and associated payments.

DESIGNATION OF FIRST VIRTUAL CURRENCY EXCHANGE FOR COMPLICIT FINANCIAL SERVICES

Today's actions include the Department of the Treasury's Office of Foreign Assets Control's (OFAC) designation of SUEX OTC, S.R.O. (SUEX), a virtual currency exchange, for its part in facilitating financial transactions for ransomware actors. SUEX has facilitated transactions involving illicit proceeds from at least eight ransomware variants. Analysis of known SUEX transactions shows that over 40% of SUEX's known transaction history is associated with illicit actors. SUEX is being designated pursuant to Executive Order 13694, as amended, for providing material support to the threat posed by criminal ransomware actors.

Virtual currency exchanges such as SUEX are critical to the profitability of ransomware attacks, which help fund additional cybercriminal activity. Treasury will continue to disrupt and hold accountable these entities to reduce the incentive for cybercriminals to continue to conduct these attacks. This action is the first sanctions designation against a virtual currency exchange and was executed with assistance from the Federal Bureau of Investigation.

While most virtual currency activity is licit, virtual currencies can be used for illicit activity through peer-to-peer exchangers, mixers, and exchanges. This includes the facilitation of sanctions evasion, ransomware schemes, and other cybercrimes. Some virtual currency exchanges are exploited by malicious actors, but others, as is the case with SUEX, facilitate illicit activities for

their own illicit gains. Treasury will continue to use its authorities against malicious cyber actors in concert with other U.S. departments and agencies, as well as our foreign partners, to disrupt financial nodes tied to ransomware payments and cyber-attacks. Those in the virtual currency industry play a critical role in implementing appropriate AML/CFT and sanctions controls to prevent sanctioned persons and other illicit actors from exploiting virtual currencies to undermine U.S foreign policy and national security interests.

SANCTIONS IMPLICATIONS

As a result of today's designation, all property and interests in property of the designated target that are subject to U.S. jurisdiction are blocked, and U.S. persons are generally prohibited from engaging in transactions with them. Additionally, any entities 50% or more owned by one or more designated persons are also blocked. In addition, financial institutions and other persons that engage in certain transactions or activities with the sanctioned entities and individuals may expose themselves to sanctions or be subject to an enforcement action. Today's action against SUEX does not implicate a sanctions nexus to any particular Ransomware-as-a-Service (RaaS) or variant.

OFAC UPDATES ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS

OFAC today also released an Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments . The Advisory emphasizes that the U.S. government continues to strongly discourage the payment of cyber ransom or extortion demands and recognizes the importance of cyber hygiene in preventing or mitigating such attacks. OFAC has also updated the Advisory to emphasize the importance of improving cybersecurity practices and reporting to, and cooperating with, appropriate U.S. government agencies in the event of a ransomware attack. Such reporting, as the Advisory notes, is essential for U.S. government agencies, including law enforcement, to understand and counter ransomware attacks and malicious cyber actors.

OFAC strongly encourages victims and related companies to report these incidents to and fully cooperate with law enforcement as soon as possible to avail themselves of OFAC's significant mitigation related to OFAC enforcement matters and receive voluntary self-disclosure credit in the event a sanctions nexus is later determined.

ADDITIONAL AUTHORITIES

FinCEN, in addition to the guidance and enforcement activities above, has also engaged with industry, law enforcement, and others on the ransomware threat through the FinCEN Exchange public-private partnership. FinCEN held a first Exchange on ransomware in November 2020 and a second Exchange in August 2021. FinCEN is taking additional action under its authorities to collect information relating to ransomware payments.

INTERNATIONAL COOPERATION AND IMPORTANCE OF AML/CFT MEASURES FOR VIRTUAL CURRENCIES AND SERVICE PROVIDERS

Countering ransomware benefits from close collaboration with international partners. At the Group of Seven (G7) meeting in June, participants committed to working together to urgently address the escalating shared threat from criminal ransomware networks. The G7 is considering the risks surrounding ransomware, including potential impacts to the finance sector. For example, the G7 Cyber Expert Group (CEG), co-chaired by Treasury and Bank of England, met on September 1 and September 14, 2021 to discuss ransomware, which remains a grave concern given the number and breadth of ransomware attacks across industry sectors. The participants considered the effects of ransomware attacks on the financial services sector, as well as the broader economy, and explored ways to help improve overall security and resilience against malicious cyber activity.

Given the illicit finance risk that virtual assets pose, including ransomware-related money laundering, in June 2019 the Financial Action Task Force (FATF) amended its standards to require all countries to regulate and supervise virtual asset service providers (VASPs), including exchanges, and to mitigate against such risks when engaging in virtual asset transactions. Among other things, countries are expected to impose customer due diligence (CDD) requirements, and suspicious transaction reporting obligations across VASPs, which can help inhibit cybercriminals' exploitation of virtual assets while supporting investigations into these illicit finance activities. Because profit-motivated cybercriminals must launder their misappropriated funds, AML/CFT regimens are a critical chokepoint in countering and deterring this criminal activity. This magnifies the need for all countries to effectively and expeditiously implement and enforce the FATF's standards on virtual assets and VASPs. The United States is

committed to continued work at the FATF and with other countries to implement the FATF standards, and we welcome the FATF's ongoing work on this issue.

Click here to view identifying information on the entity designated today.

Click here for OFAC's Frequently Asked Questions on Virtual Currency.

FOR MORE INFORMATION ON RANSOMWARE

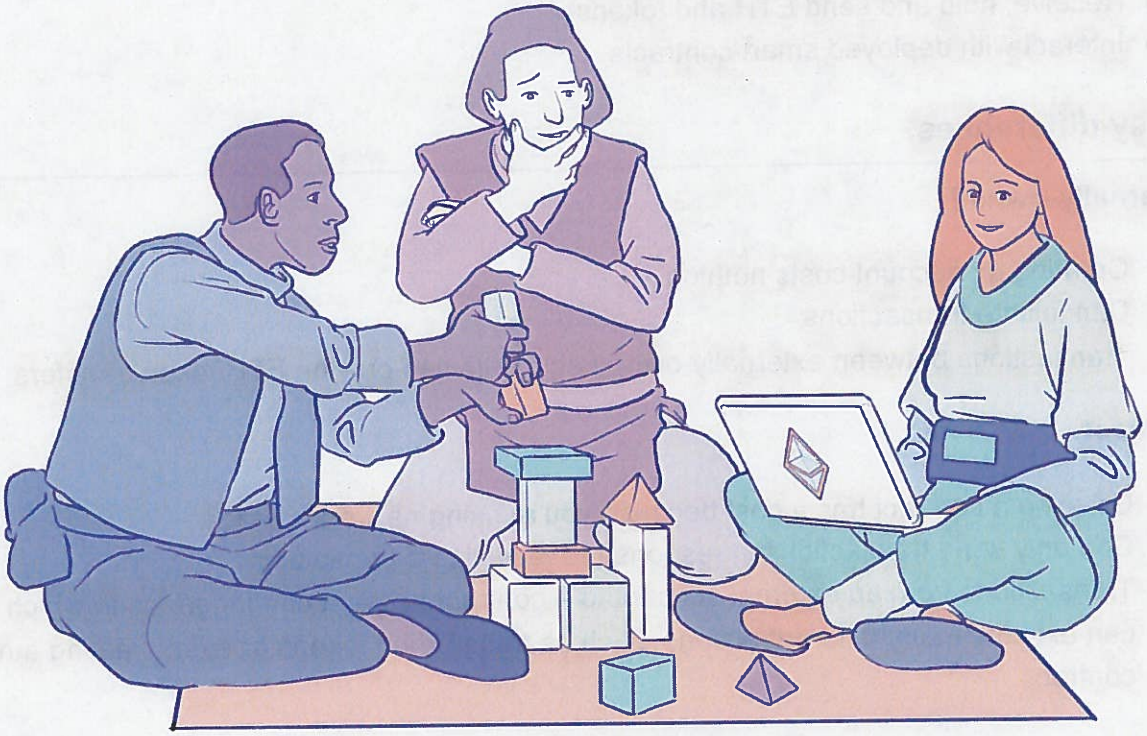
Please visit StopRansomware.gov, a one-stop resource for individuals and organizations of all sizes to reduce their risk of ransomware attacks and improve their cybersecurity resilience. This webpage brings together tools and resources from multiple federal government agencies under one online platform. Learn more about how ransomware works, how to protect yourself, how to report an incident, and how to request technical assistance.

###

EXHIBIT 58

Ethereum accounts

ethereum.org/en/developers/docs/accounts/



Last edit: , Invalid DateTime

Edit page

On this page

An Ethereum account is an entity with an ether (ETH) balance that can send transactions on Ethereum. Accounts can be user-controlled or deployed as smart contracts.

Prerequisites

Accounts are a very beginner-friendly topic. But to help you better understand this page, we recommend you first read through our introduction to Ethereum.

Account types

Ethereum has two account types:

- Externally-owned – controlled by anyone with the private keys
- Contract – a smart contract deployed to the network, controlled by code. Learn about smart contracts

Both account types have the ability to:

- Receive, hold and send ETH and tokens
- Interact with deployed smart contracts

Key differences

Externally-owned

- Creating an account costs nothing
- Can initiate transactions
- Transactions between externally-owned accounts can only be ETH/token transfers

Contract

- Creating a contract has a cost because you're using network storage
- Can only send transactions in response to receiving a transaction
- Transactions from an external account to a contract account can trigger code which can execute many different actions, such as transferring tokens or even creating a new contract

An account examined

Ethereum accounts have four fields:

- `nonce` – A counter that indicates the number of transactions sent from the account. This ensures transactions are only processed once. In a contract account, this number represents the number of contracts created by the account.
- `balance` – The number of wei owned by this address. Wei is a denomination of ETH and there are 1e+18 wei per ETH.
- `codeHash` – This hash refers to the *code* of an account on the Ethereum virtual machine (EVM). Contract accounts have code fragments programmed in that can perform different operations. This EVM code gets executed if the account gets a message call. It cannot be changed, unlike the other account fields. All such code fragments are contained in the state database under their corresponding hashes for later retrieval. This hash value is known as a codeHash. For externally owned accounts, the codeHash field is the hash of an empty string.

- `storageRoot` – Sometimes known as a storage hash. A 256-bit hash of the root node of a Merkle Patricia trie that encodes the storage contents of the account (a mapping between 256-bit integer values), encoded into the trie as a mapping from the Keccak 256-bit hash of the 256-bit integer keys to the RLP-encoded 256-bit integer values. This trie encodes the hash of the storage contents of this account, and is empty by default.

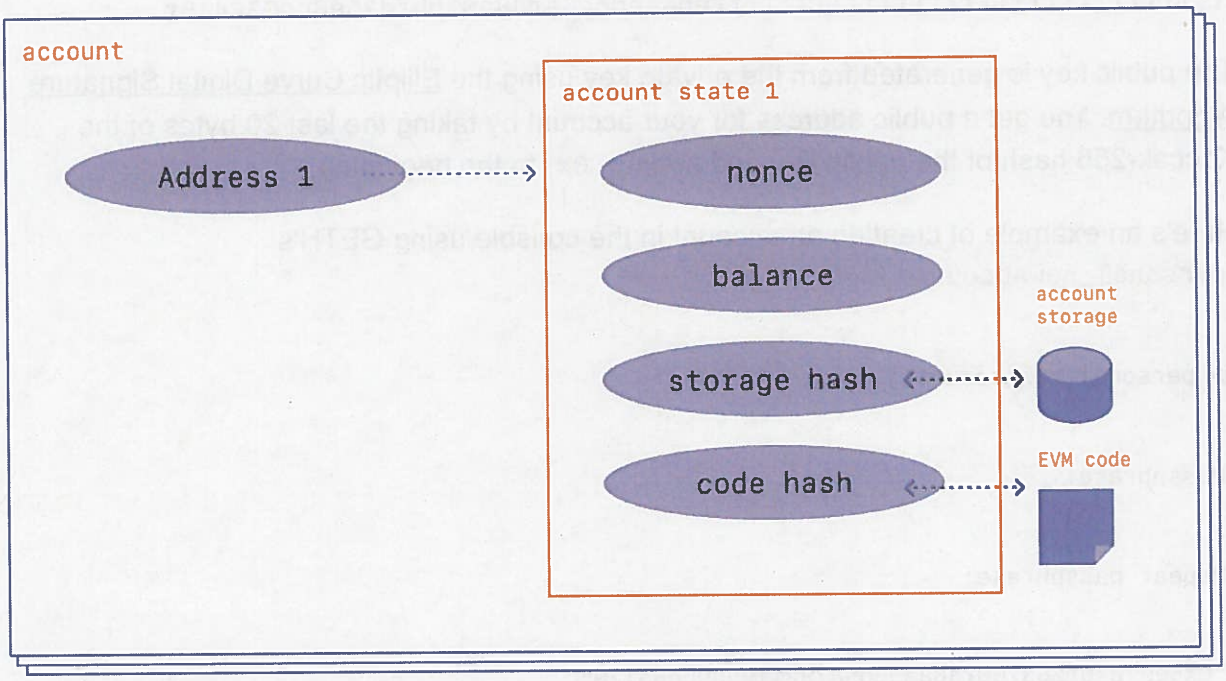


Diagram adapted from Ethereum EVM illustrated

Externally-owned accounts and key pairs

An account is made up of a cryptographic pair of keys: public and private. They help prove that a transaction was actually signed by the sender and prevent forgeries. Your private key is what you use to sign transactions, so it grants you custody over the funds associated with your account. You never really hold cryptocurrency, you hold private keys – the funds are always on Ethereum's ledger.

This prevents malicious actors from broadcasting fake transactions because you can always verify the sender of a transaction.

If Alice wants to send ether from her own account to Bob's account, Alice needs to create a transaction request and send it out to the network for verification. Ethereum's usage of public-key cryptography ensures that Alice can prove that she originally initiated the transaction request. Without cryptographic mechanisms, a malicious adversary Eve could simply publicly broadcast a request that looks something like "send 5 ETH from Alice's account to Eve's account," and no one would be able to verify that it didn't come from Alice.

Account creation

When you want to create an account most libraries will generate you a random private key.

A private key is made up of 64 hex characters and can be encrypted with a password.

Example:

`ffffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd036415f`

The public key is generated from the private key using the Elliptic Curve Digital Signature Algorithm. You get a public address for your account by taking the last 20 bytes of the Keccak-256 hash of the public key and adding `0x` to the beginning.

Here's an example of creating an account in the console using GETH's `personal_newAccount`

```
1> personal.newAccount()

2Passphrase:

3Repeat passphrase:

4"0x5e97870f263700f46aa00d967821199b9bc5a120"

5


6> personal.newAccount("h4ck3r")

7"0x3d80b31a78c30fc628f20b2c89d7ddbf6e53cedc"

8
```

GETH documentation

It is possible to derive new public keys from your private key but you cannot derive a private key from public keys. This means it's vital to keep a private key safe and, as the name suggests, **PRIVATE**.

You need a private key to sign messages and transactions which output a signature. Others can then take the signature to derive your public key, proving the author of the message. In your application, you can use a javascript library to send transactions to the network.

Contract accounts

Contract accounts also have a 42 character hexadecimal address:

Example:

```
0x06012c8cf97bead5deae237070f9587f8e7a266d
```

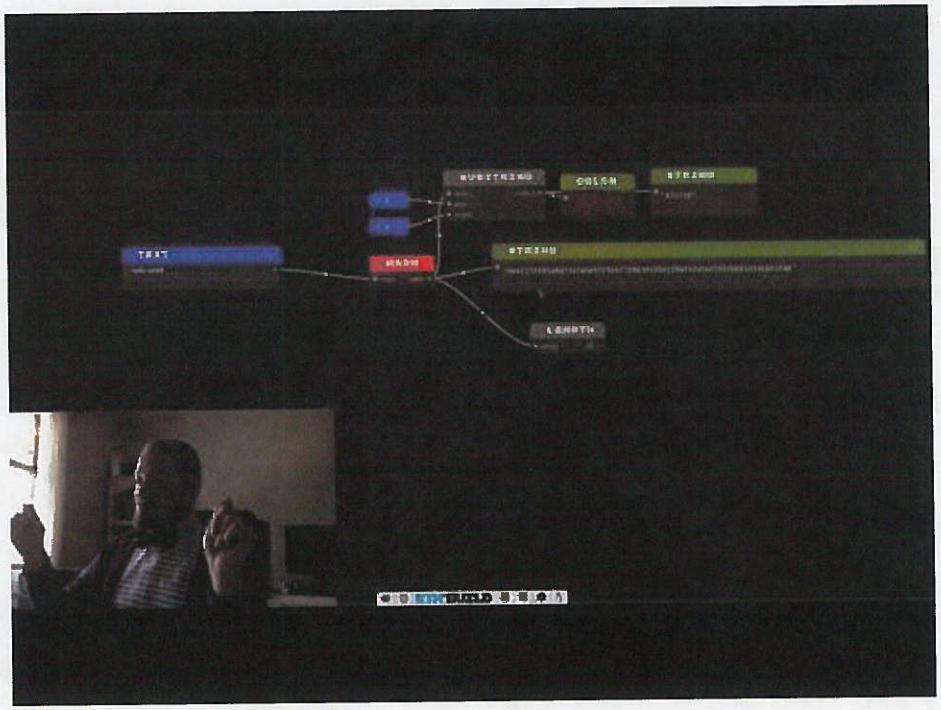
The contract address is usually given when a contract is deployed to the Ethereum Blockchain. The address comes from the creator's address and the number of transactions sent from that address (the “nonce”).

A note on wallets

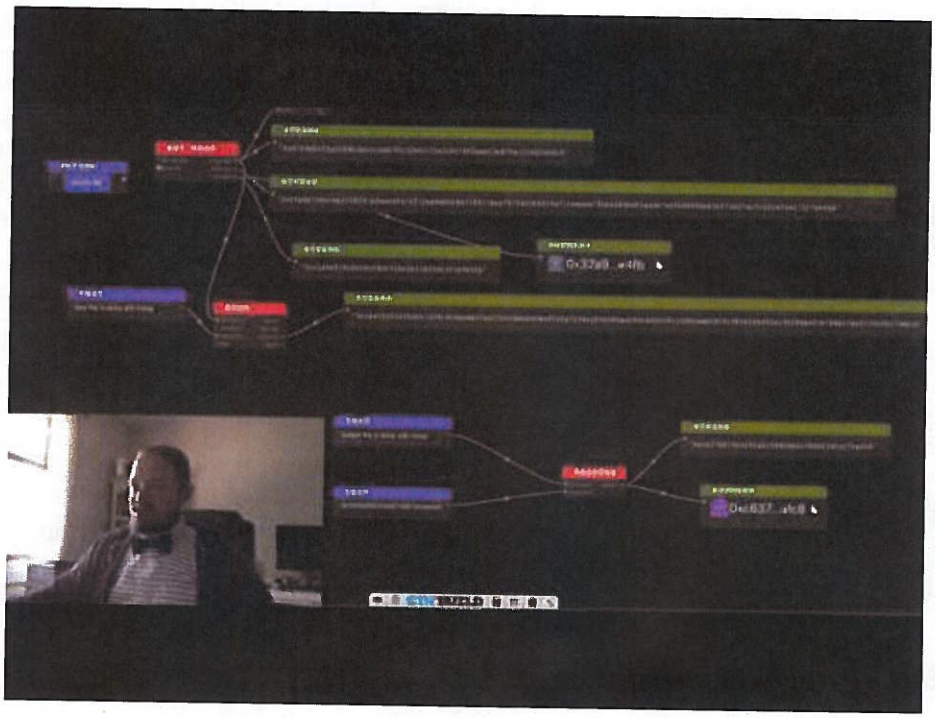
An account is not a wallet. An account is the keypair for a user-owned Ethereum account. A wallet is an interface or application that lets you interact with your Ethereum account.

A visual demo

Watch Austin walk you through hash functions, and key pairs.



Watch Video At: https://youtu.be/QJ010l-pBpE



Watch Video At: https://youtu.be/9LtBDy67Tho

Further reading

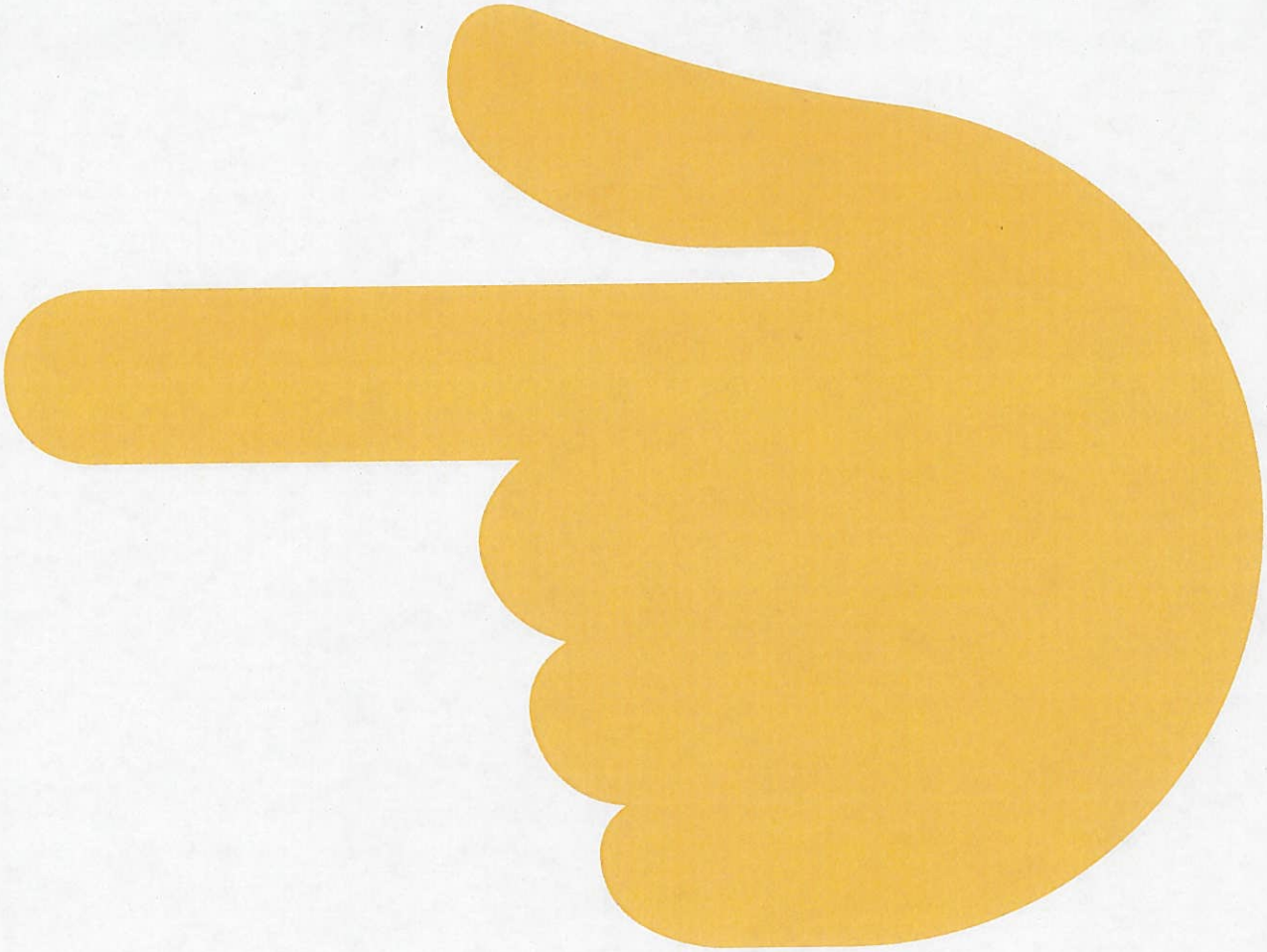
Know of a community resource that helped you? Edit this page and add it!

Related topics

- Smart contracts
- Transactions

Back to top ↑

Was this article helpful?



PreviousWeb2 vs Web3
NextTransactions

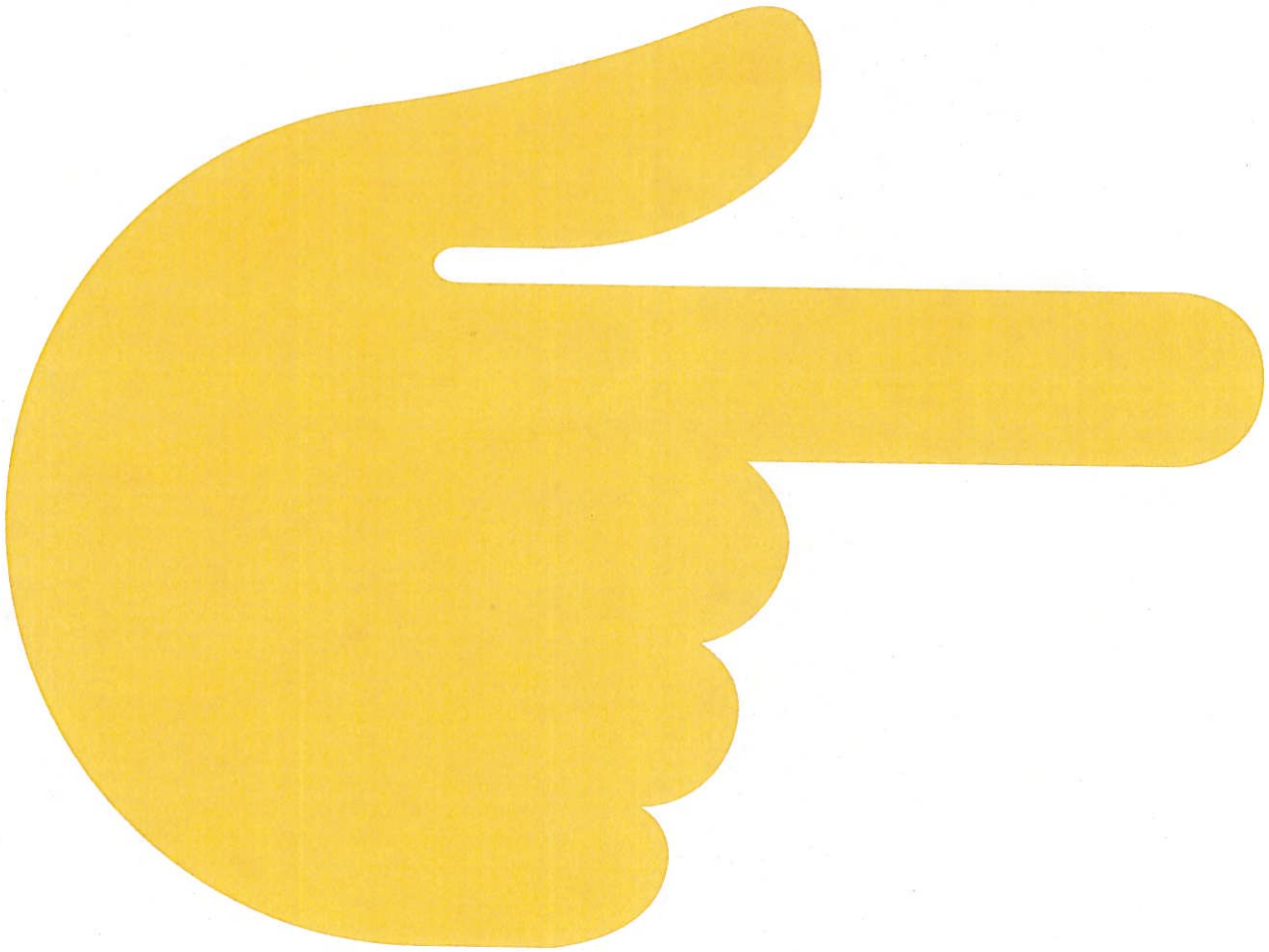


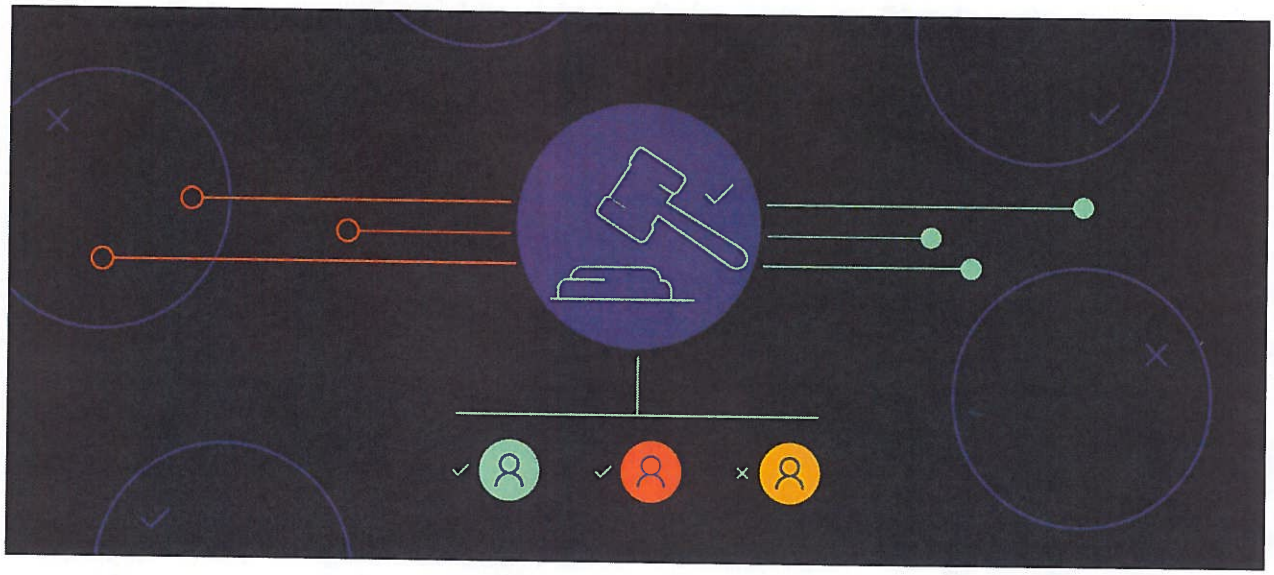
EXHIBIT 59

Dissecting the DAO: Web3 Ownership is Surprisingly Concentrated

blog.chainalysis.com/reports/web3-daos-2022/

Chainalysis Team

June 27, 2022



This blog is a preview of our State of Web3 Report. Sign up here to download your copy!

Decentralized autonomous organizations (DAOs) are a staple of web3. Internet-native and blockchain-based, DAOs are intended to provide a new, democratized management structure for businesses, projects, and communities, in which any member can vote on organizational decisions just by buying into the project.

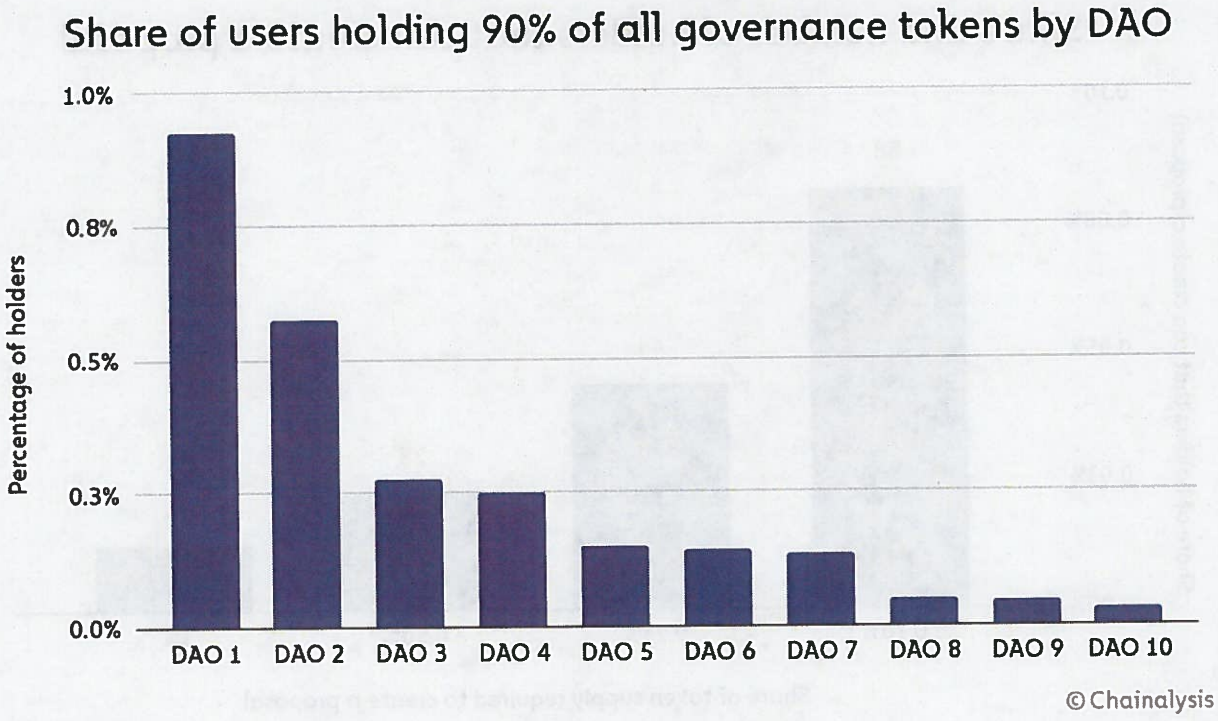
At a high level, this is how DAOs work:

1. DAO founders create a new cryptocurrency, known as a **governance token**;
2. They distribute these tokens to users, backers, and other stakeholders;
3. Each token corresponds to a set amount of voting power within the organization. It also corresponds to a price on the secondary market, where it can be bought and sold at will.

While this process is often described as a way to decentralize power, governance token data suggests that DAO ownership is highly concentrated.

The concentration of governance token holdings

By analyzing the distribution of ten major DAOs' governance tokens, we find that, across several major DAOs, less than 1% of all holders have 90% of the voting power.



This has meaningful implications for DAO governance. For example, if just a small portion of the top 1% of holders worked together, they could theoretically outvote the remaining 99% on any decision. This has obvious practical implications and, in terms of investor sentiment, likely affects whether small holders feel that they can meaningfully contribute to the proposal process.

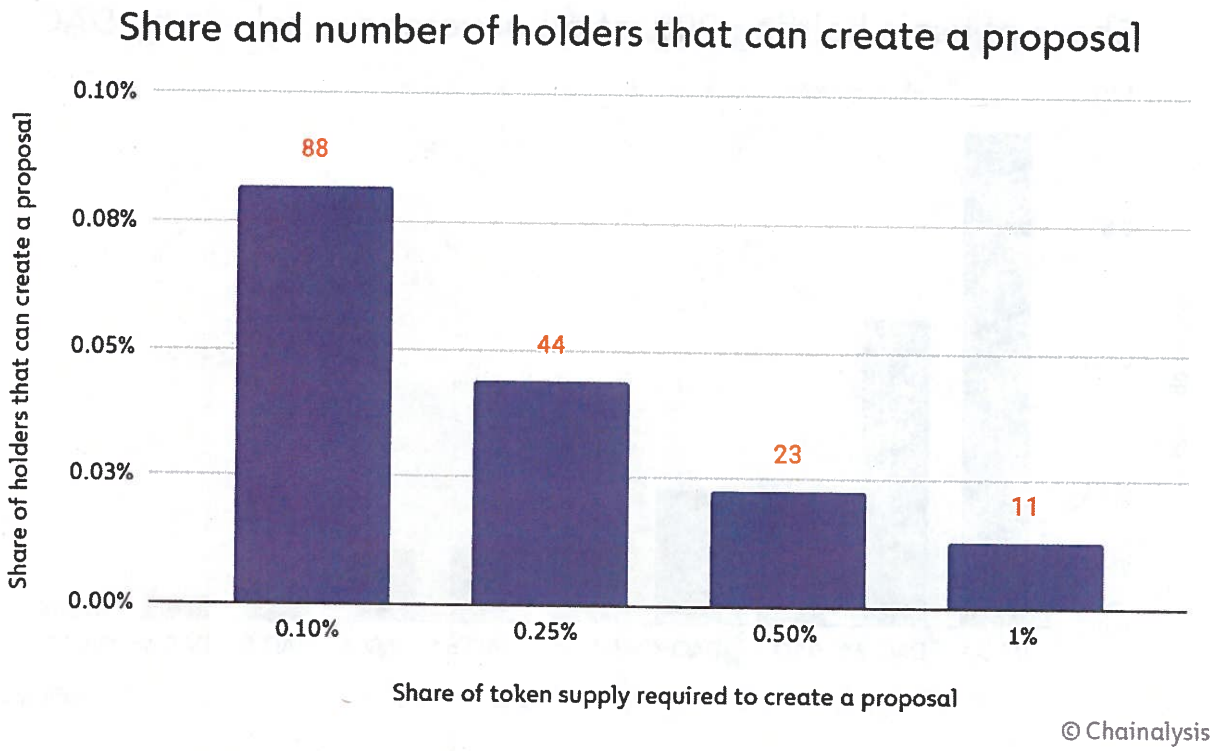
The impact of high concentration on DAO governance

For a governance token holder, there are three key governance actions. Voting is simple – any holder can do it. But what about creating a proposal? And what about passing it?

Per these ten DAOs proposal requirements, we find that:

1. A user must hold between 0.1% and 1% of the outstanding token supply to create a proposal.
2. A user must hold between 1% and 4% to pass it.

Using these ranges as lower and upper bounds, we find that **between 1 in 1,000 and 1 in 10,000 of these ten DAOs' holders have enough tokens to create a proposal**.



There are several tradeoffs at play here. If too many holders can create a proposal, the average proposal's quality may fall, and the DAO may be riddled with governance spam. But if too few can, the community may come to feel that "decentralized governance" rings false.

When it comes to single-handedly *passing* a proposal, **between 1 in 10,000 and 1 in 30,000 holders have enough tokens to do so**.

Overly concentrated voting power in DAOs can result in decision-making that seemingly contradicts the tenets of decentralization on which web3 is built. For instance, in June 2022, the DAO governing the Solana-based lending protocol Solend faced a problem: Solana's price was dropping, and if it fell much further, the protocol's biggest whale user would face a margin call that could render Solend insolvent and send roughly $20 million worth of Solana onto the market, potentially tanking the asset's price and upending the entire Solana ecosystem. The DAO called a vote to take control of the whale's account and liquidate its position through OTC desks, rather than the open market.

> Governance proposal SLND1 has passed.
>
> Special margin requirements for accounts that represent over 20% of borrows are now in effect.
>
> There will be a grace period for 3oSE…uRbE to reduce their leverage by themselves. pic.twitter.com/dsZhFRC8ZX
>
> — Solend (we're hiring!) (@solendprotocol) June 19, 2022

The proposal passed easily, with over 1.1 million "yes" votes to 30,000 "no" votes. However, more than 1 million of those votes came from a single user with enormous governance token holdings. Without their vote, the motion wouldn't have passed the 1% participation rate necessary for quorum.

The decision triggered a backlash from the cryptocurrency community, with many questioning how a platform could claim to be decentralized and then take control of a user's funds against their will. Following this, the Solend DAO voted again to invalidate the proposal, and the whale user eventually began to unwind their position. While the crisis was averted in this case, it raises questions about the ability of a DAO to act in the best interest of all participants when some voters control such an outsized share of governance tokens.

How do DAOs govern, exactly?

Actual governance processes vary enough from DAO to DAO that this question is best answered with examples. Let's start with the biggest one: Uniswap.

Example: Uniswap Governance

Uniswap is a decentralized exchange (DEX), and, like many DeFi protocols, it is governed by a DAO.

Anyone who holds Uniswap's governance token, UNI, is a member of this DAO. They can participate in governance by delegating their voting rights to their own or another's address, by publicizing their opinions, or by submitting their own proposal. The contents of these proposals vary widely: holders have recently voted on whether to finance a grant program, whether to integrate a new blockchain, and whether to reduce the governance proposal submission threshold.

But before someone can submit a proper proposal, their idea must pass the first two phases: temperature checks and consensus checks.

1. **The temperature check** determines whether there is sufficient community will to change the status quo. At the end of the two days, a majority vote with a 25,000 UNI yes-vote threshold wins.
2. **The consensus check** establishes formal discussion around a potential proposal. At the end of five days, a majority vote with a 50,000 UNI yes-vote threshold wins.

If both checks pass, an official governance proposal can be put to a vote. Then, there's a seven-day deliberation period to discuss the merits of this proposal on governance forums. If at the end of this period there are at least 40 million yes-votes with no-votes as a minority, the proposal has passed, and will be enacted after a two-day timelock.

Example: Dream DAO Governance

Not all DAOs function like Uniswap, but most at least run on similar infrastructure, using voting systems like Snapshot and chat servers like Discord. Dream DAO is no exception, though its mission and therefore its governance process is necessarily unique.

Dream DAO is an impact-oriented DAO created by 501(c)(3) charity Civics Unplugged and designed to provide diverse Gen Zers globally with the training, funding, and community they need to use web3 to improve humanity. Their governance process is run by holders of SkywalkerZ – NFTs that function as both governance tokens and fundraising incentives for anyone interested in donating to the program. For every SkywalkerZ NFT purchased by a donor, a new SkywalkerZ is reserved for a future Gen Zer to join as a voting member, thereby receiving power in the DAO without needing to pay. The purchaser of the NFT can apply to join the DAO and become a voting member as well, or they can leave it to the Gen Z student they've sponsored — either way, the NFT is theirs to keep.

By removing financial barriers from the process of participating in DAO governance, Dream DAO empowers its target audience – future Gen Z leaders – to influence decision-making, immerse themselves in web3, and leverage blockchain technologies positively.

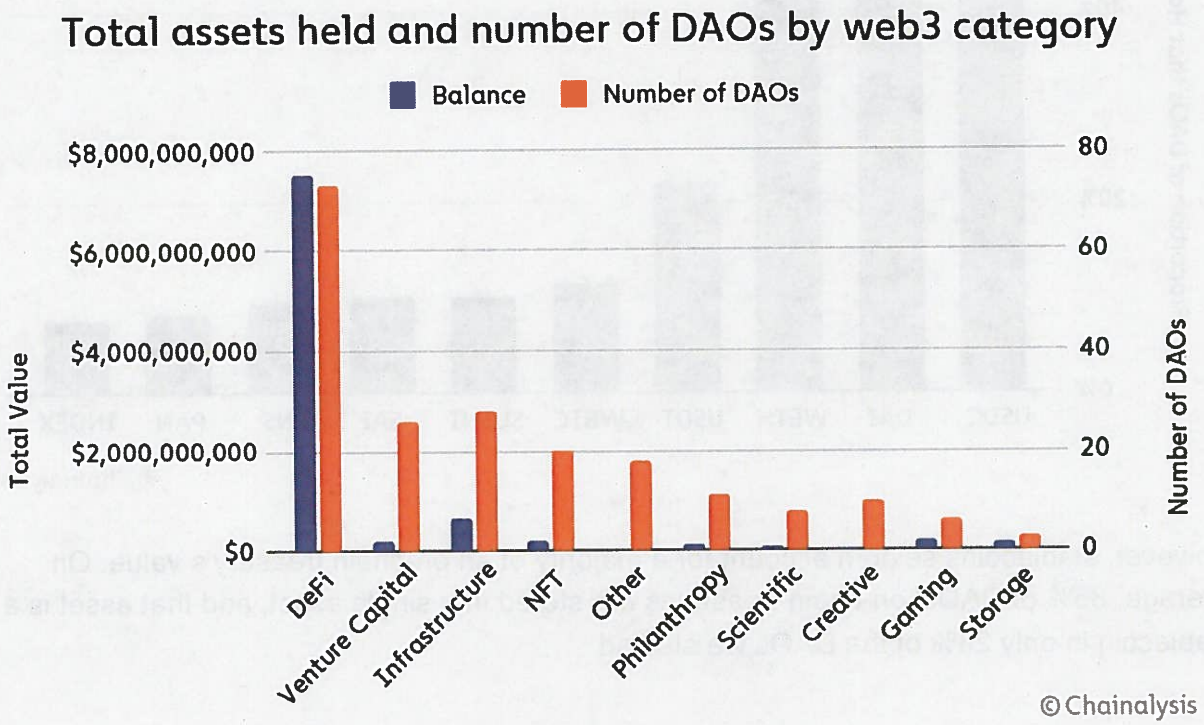
Where are DAOs most common and well-funded?

DAOs span the entire length of web3. They govern:

- **DeFi protocols** like Uniswap ($UNI) and Sushi ($SUSHI).
- **Social clubs** like Friends With Benefits ($FWB) and Bored Ape Yacht Club ($APE).
- **Grant-makers** like Gitcoin ($GTC) and Seed Club ($CLUB).
- **Play-to-earn gaming guilds** like Good Games Guild ($GGG) and Yield Guild Games ($YGG).
- **NFT generators** like Nouns (1 NFT = 1 vote).
- **Venture funds** like MetaCartel and Orange DAO.
- **Charities** like Big Green DAO and DreamDAO (1 SkywalkerZ = 1 vote).

- **Virtual worlds** like Decentraland ($MANA) and Sandbox ($SAND) .
- **And more**.

But in terms of raw numbers and treasury sizes, DeFi-related DAOs have a giant lead. The DeFi category accounts for 83% of all DAO treasury value held and 33% of all of the DAOs by count.

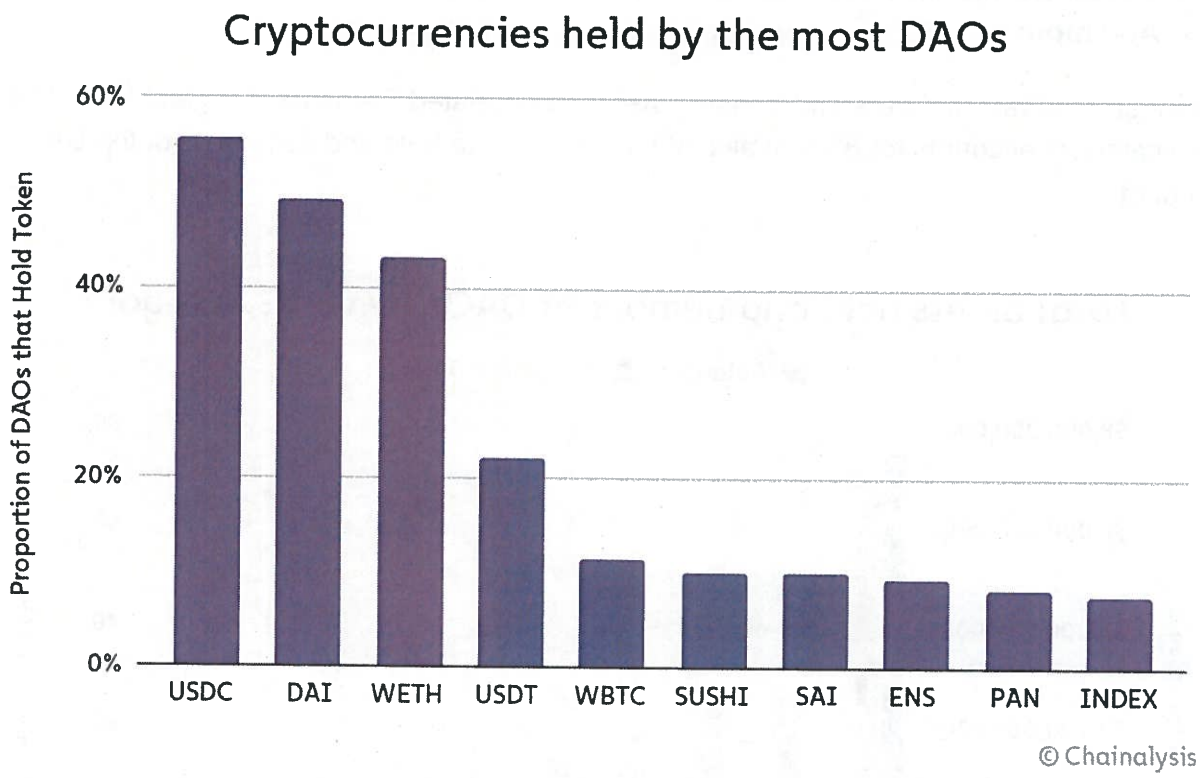


There are also a large number of DAOs focused on venture capital, infrastructure, and NFTs, suggesting that DAOs are appealing to investors, developers, and artists. Their on-chain treasuries, however, are relatively tiny.

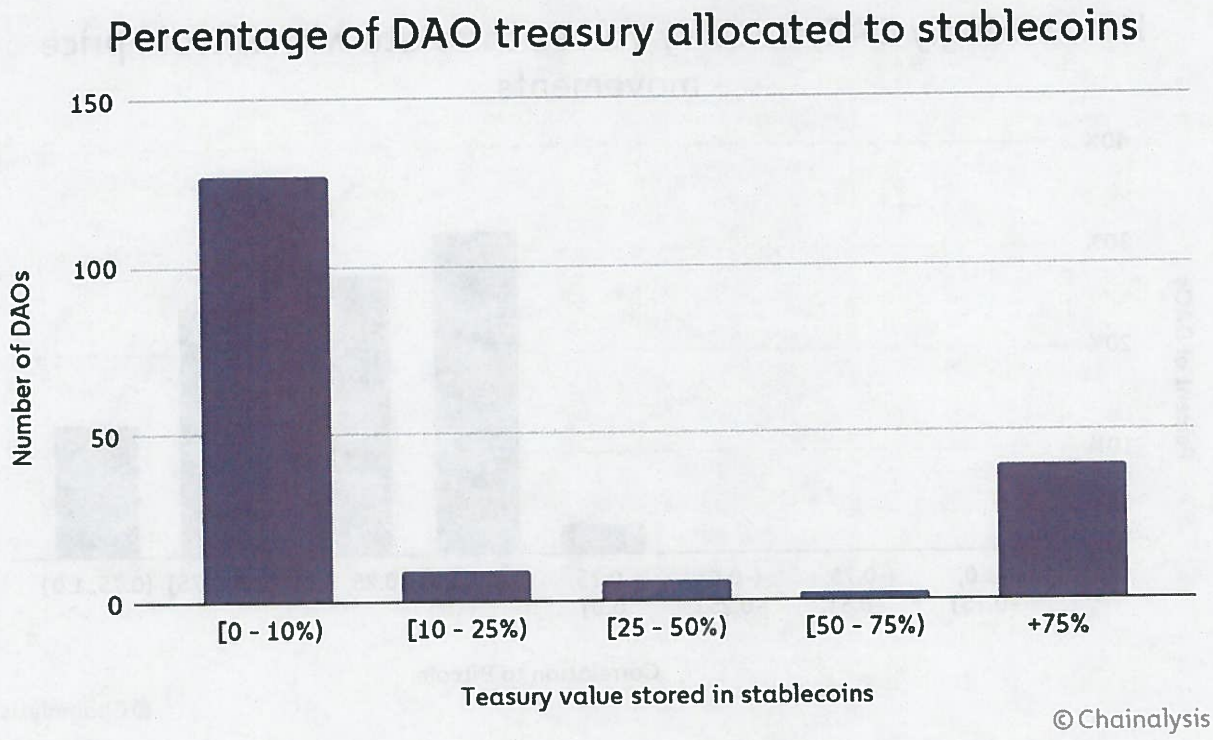
To be fair, the lines between these categories are blurry. Gaming DAOs often engage with NFTs, venture DAOs often provide funding to DeFi, and infrastructure DAOs support all of the above categories.

Treasury management: What assets do DAOs hold?

Even though DAOs vary in type and size, most of their on-chain treasuries hold similar cryptocurrencies. The most commonly held cryptocurrency is the stablecoin USD Coin (USDC), with over half of the 197 DAOs we analyzed holding a balance of USDC.



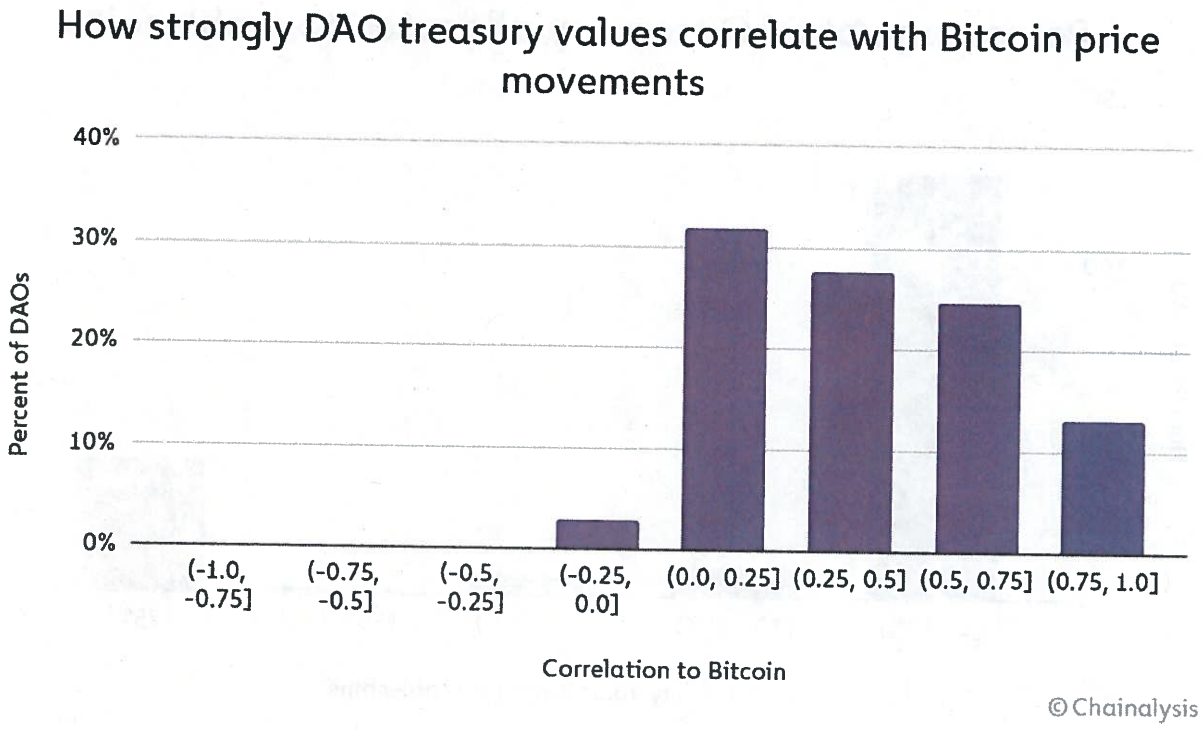
However, stablecoins seldom account for a majority of an on-chain treasury's value. On average, 85% of DAOs' on-chain treasuries are stored in a single asset, and that asset is a stablecoin in only 23% of the DAOs we studied.



These on-chain treasuries are roughly as volatile as Bitcoin. By assuming DAOs' current holdings are their historical portfolios over the past year, we find that:

- The average DAO with assets over $1 million has an annualized volatility of 82%, versus 69% for Bitcoin.
- The average DAO with assets over $1 million suffered a maximum drawdown of 51% over the past year, compared to Bitcoin's drawdown of 72%.

DAO treasury values are also fairly correlated with Bitcoin price movements. 38% of on-chain DAO treasuries have correlations with Bitcoin that are between 0.5 and 1.00.

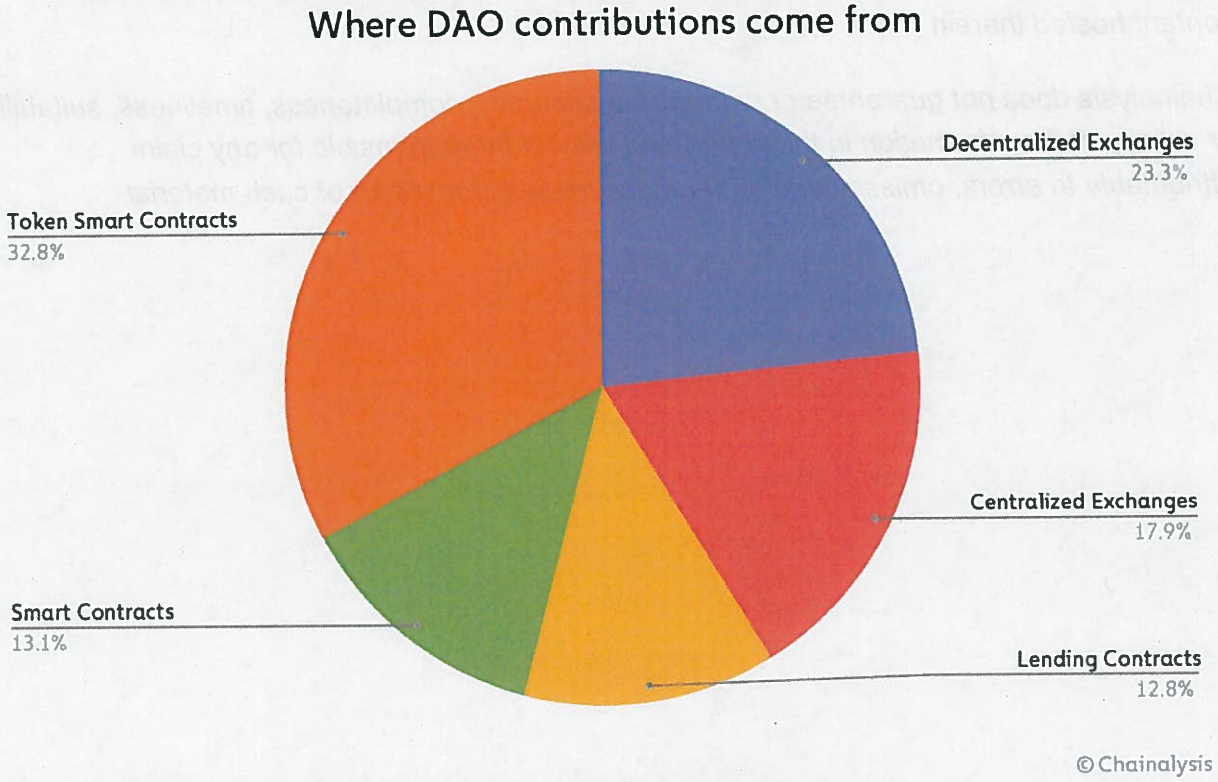


One of the most interesting areas of DAO treasury management that has yet to take off is in mergers and acquisitions (M&A). M&A makes sense for DAOs because it allows them to get into adjacent areas without having to develop internal tooling. As the DAO model matures, we suspect M&A will become more commonplace.

DAOs thus far have also been fairly limited in terms of the types of instruments they use and hold. For example, few DAOs to date have used loans or credit, perhaps due to their uncertain legal status. As DAOs mature, we are likely to see more standardized regulations, management strategies, and reporting practices.

Who contributes to DAOs?

While we don't collect demographic data about DAO participants, we can learn some things about DAO contributors using blockchain data.



Token smart contract = a project-specific ERC-20 or Layer 1 token contract

As one might expect, DAO participants are advanced users of cryptocurrency services. Only 17.9% of DAO treasury funds came from centralized services, while the remaining 82.1% originated at decentralized services. This suggests that most DAO contributors also engage with DeFi platforms and likely self-host their cryptocurrency.

The future of DAOs

As DAOs gain momentum, a cottage industry of tooling services and advocacy groups have emerged to help them grow and govern. Superdao streamlines DAO creation; Snapshot simplifies governance; and Coin Center advocates for the industry on Capitol Hill. As they continue to expand, it will be interesting to see what they can accomplish, what they will become, and to what extent they will achieve their goal to decentralize the ownership of the internet. With the proliferation of DAOs today, we'll have plenty of chances to see.

Download the State of Web3 Report

This website contains links to third-party sites that are not under the control of Chainalysis, Inc. or its affiliates (collectively "Chainalysis"). Access to such information does not imply association with, endorsement of, approval of, or recommendation by Chainalysis of the site

or its operators, and Chainalysis is not responsible for the products, services, or other content hosted therein.

Chainalysis does not guarantee or warrant the accuracy, completeness, timeliness, suitability or validity of the information in this report and will not be responsible for any claim attributable to errors, omissions, or other inaccuracies of any part of such material.

EXHIBIT 61

Tornado Cash Follow
Dec 18, 2020 · 9 min read

Tornado.Cash Governance Proposal

Tornado.Cash has become the largest privacy solution on Ethereum today. Tornado.Cash has been fully autonomous and decentralized, but it's static — it has no way to evolve. This is a proposal to change that. If this proposal is adopted, then the governance of Tornado.Cash will be entrusted to its users, and Tornado.Cash will be allowed to evolve under the stewardship of its community. This way, the users of Ethereum will control their own privacy protocol.

Here is how a proposal for how the Tornado.Cash governance system could work:

TORN Token

TORN is an ERC20-compatible token with a fixed supply that governs Tornado.Cash. TORN holders can make proposals and vote to change the protocol via governance.

TORN is not a fundraising device or investment opportunity. It will remain non-transferable until the community decides that unlocking transfers via a governance vote, not earlier than 45 days following deployment, would comply with all applicable laws.

Here's how the initial distribution of TORN would break down:

- **5% (500,000 TORN):** Airdrop to early users of Tornado.Cash ETH pools
- **10% (1,000,000 TORN):** Anonymity mining for Tornado.Cash ETH pools, distributed linearly over 1 year

- **30% (3,000,000 TORN):** Founding developers and early supporters, will be unlocked linearly over 3 years with 1 year cliff

Airdrop

Users who have believed in Tornado.Cash from early on should have a say in governing the protocol. For this reason, early adopters of the protocol will receive an airdrop of TORN.

TORN will be airdropped to all addresses that made deposits into Tornado.Cash ETH pools before block `11400000`. TORN will be airdropped in the form of a non-transferable TORN voucher (vTORN) that can be redeemed 1:1 to TORN within 1 year. TORN that aren't redeemed will be swept into the governance contract after 1 year and become part of the DAO Treasury. Redeemed TORN will be available immediately.

The airdropped amount depends on users' deposit size and age — larger deposits and older deposits will receive more TORN. Multipliers for deposit size are logarithmic:

So a 100 ETH deposit will get twice as many tokens as a 1 ETH deposit. The multiplier allows large and small users of Tornado.Cash to both have a say in governance.

The exact curve for the time multiplier looks like this:

The exact airdrop formula is the following:

Anonymity Mining

The fundamental principle behind Tornado.Cash is that privacy is a human right, and the more everyone adopts privacy measures, the more secure it is for all of us (much like how HTTPS becoming the default for web browsers made all of us more secure). To this end, users who add to the anonymity set of Tornado.Cash in the future should also receive TORN

spent in a Tornado.Cash pool. This conflicts with Tornado.Cash's core value: preserving privacy.

That is the driving impetus behind the invention of **Anonymity Mining.** In Anonymity Mining, users will be able to receive TORN through a two-stage shielded liquidity mining system, which fully preserves user privacy.

After a user deposits into Tornado.Cash, a user will accrue private **Anonymity Points** (AP) into a shielded account — which shields your wallet address, your balance, and doesn't leak any information about your deposits. Once the user accumulates enough AP on the user's shielded account, the user can decide to convert the AP at any time into public TORN tokens via our custom-built Tornado.Cash AMM.

This system is a little complex. But it ensures that user privacy is always protected in the process of claiming TORN tokens.

Note: only notes that are deposited **after the deployment ceremony** are eligible for Anonymity Mining — earlier notes are distributed TORN via the airdrop.

Here's how it works, step-by-step:

Claiming your AP

First, users must claim Anonymity Points (AP) for *already spent* Tornado.Cash notes (AP cannot be claimed until the user spends the notes). After the notes are spent, there is delay before it becomes claimable for AP.

To claim AP, the user's browser generates a special zero knowledge proof that calculates the AP owed (based on how many blocks the user's note was in an ETH Tornado.Cash pool) and then adds that to the user shielded balance. Below is a table of AP per block for different Tornado.Cash note sizes:

The only information other users will see on-chain is that *someone* claimed some AP batch of unknown size for *some* note for a certain Tornado.Cash pool. To further enhance privacy, the user can claim AP via a relayer (who will accept AP as compensation to cover their relaying costs).

Shielded Accounts

Because AP is completely private, in order to store your shielded AP, the user needs to generate a secret key that stores the user's AP balance. This key is randomly generated, and then encrypted with your Ethereum public key (using Metamask's `eth_getEncryptionPublicKey`) and stored on-chain. That way, if you lose it, it can be seamlessly recovered using the user's Ethereum keys.

This secret key is used to encrypt and submit claim and withdrawal data without revealing the user's identity.

Converting AP into TORN

To then convert your mined AP into publicly visible TORN, you can use the custom-built Tornado.Cash Automated Market Maker (AMM).

TORN is dripped continuously and evenly into this AMM (1M TORN tokens over 1 year). All the AP that is claimed at any point can bid on the TORN that has up to that point accumulated in the AMM.

This does mean that the timing to convert AP into TORN is somewhat strategic — if too

Here's a rough analogy: you can imagine TORN tokens are being released by a drip into a bucket (the AMM) over one year. AP tokens let you bid on whatever amount of TORN is in the bucket so far. If there's a lot of AP bidding at the same time, the bucket will drain really quickly and the rate per AP will be low. But if the AP holders are patient, it should level out over time and everyone should get a roughly equal number of TORN for AP.

That's the entire process for claiming TORN. Unfortunately there's some irreducible complexity. But, it's impossible to know how much AP will get generated over the course of the Anonymity Mining program (since it's private!), so this is the only way to ensure both that TORN has a fixed supply and that all AP remains shielded until it is converted into public TORN.

The exact AMM formula looks like this:

where:

- T — TORN mining program allocation
- $Tvirt$ — Virtual TORN balance
- $Twithdrawn$ — Amount of TORN that users already withdrawn
- $TORN$ — Amount of TORN that user will receive
- AP — Anonymity points to exchange
- W — AMM exchange weight constant

The Tornado Cash Proxy

It is! The Tornado.Cash smart contracts cannot be changed or updated. They are decentralized and immutable.

But for Tornado.Cash to enable mining, it needs more metadata than is currently available: it needs to know the block number for each Tornado.Cash deposit and withdrawal. To that end, a proxy stands in front of the old Tornado.Cash that adds the current block number to each transaction. Thus, for Tornado.Cash users using the proxy, their notes can be used for Anonymity Mining, since the Merkle tree will contain data about when their deposits took place. (The version of Tornado.Cash without a proxy remains fully functional.)

Note: in order to aggregate deposits and withdrawal to the Merkle trees, someone needs to run a script called the `root-updater`. So long as someone out there does this, the system works smoothly and trustlessly. Who handles this role and how it is handled is a decision for the community via governance. For more information on how this works, please check out this repo.

Governance

In order to participate in Tornado.Cash governance, users first need to lock tokens in the governance contract. If a user votes or creates a proposal, the tokens cannot be unlocked before the proposal execution period ends (8.25 days from proposal creation). The locked tokens can also be delegated to another address.

To create a proposal, a user needs to have at least 1,000 TORN. All proposals must be smart contracts with verified code that are executed from the governance contract (using `delegatecall`). This way, it's easy to audit and test any governance changes.

The voting period for a proposal is 3 days. A proposal will succeed if it receives a simple majority of votes and there are at least `25,000 TORN` total votes (if turnout is too low, the proposal automatically fails).

After a proposal succeeds, it is subject for a timelock of 2 days. After the timelock, any

All of these initial parameters are relatively small, since there won't be many TORN tokens in circulation early on. But as the circulating supply increases, governance may adjust these thresholds.

Governance proposals have the power to change any of Tornado.Cash's internal parameters, including completely upgrading its implementation (via the proxy, of course).

This brings us to...

Governance Initiation

At the end of the day, this is just a proposal. We don't control Tornado.Cash — its users do, so if the community adopts this proposal, then it will become the way forward for privacy on Ethereum.

We've written the code, and have published it to GitHub and IPFS.

The GitHub source code can be found at: torn-token, tornado-anonymity-mining, tornado-governance, tornado-initiation-ui. The proposed code is on IPFS with hash **QmR3YK3z10kFmfWNhLjGSsdJgUJJRn2NEA7NpeQEAzAi1E**, it can be accessed using a convenient shortcut **initiation.tornado.cash**. Any user can submit deploy transaction for any contract using their Metamask. It uses the CREATE2 and EIP-2470 deployer so all contract addresses are deterministic. The expected addresses of our proposed contracts are:

- **deployer.contract.tornadocash.eth**: 0xCEe71753C9820f063b38FDbE4cFDAf1d3D928A80
- **torn.contract.tornadocash.eth**:

- **governance.contract.tornadocash.eth**: 0x5efda50f22d34F262c29268506C5Fa42cB56A1Ce
- **reward-verifier.contract.tornadocash.eth**: 0x88fd245fEdeC4A936e700f9173454D1931B4C307
- **withdraw-verifier.contract.tornadocash.eth**: 0x09193888b3f38C82dEdfda55259A82C0E7De875E
- **tree-update-verifier.contract.tornadocash.eth**: 0x653477c392c16b0765603074f157314Cc4f40c32
- **reward-swap.contract.tornadocash.eth**: 0x5cab7692D4E94096462119ab7bF57319726Eed2A
- **poseidon2.contract.tornadocash.eth**: 0x94C92F096437ab9958fC0A37F09348f30389Ae79
- **poseidon3.contract.tornadocash.eth**: 0xD82ed8786D7c69DC7e052F7A542AB047971E73d2
- **tornado-proxy.contract.tornadocash.eth**: 0x905b63Fff465B9fFBF41DeA908CEb12478ec7601
- **tornado-trees.contract.tornadocash.eth**: 0x43a3bE4Ae954d9869836702AFd10393D3a7Ea417
- **mining-v2.contract.tornadocash.eth**: 0x746Aebc06D2aE31B71ac51429A19D54E797878E9
- **voucher.contract.tornadocash.eth**: 0x3eFA30704D2b8BBAc821307230376556cF8CC39e
- **team1.vesting.contract.tornadocash.eth**: 0x5f48C2A71B2CC96e3F0CCae4E39318Ff0dc375b2

- **team3.vesting.contract.tornadocash.eth**: 0x77C08248c93Ab53Ff734AC555C932F8b9089D4C9
- **team4.vesting.contract.tornadocash.eth**: 0xc3877028655EbE90b9447DD33De391c955eAd267
- **team5.vesting.contract.tornadocash.eth**: 0xb43432eC23e228FB7cB0fA52968949458b509f4F
- **governance.vesting.contract.tornadocash.eth**: 0x179f48C78f57A3A78f0608cC9197B8972921d1D2

Audit status

We thank everyone who helped us to ensure that the tornado.cash smart contracts are secure:

- ABDK (1, 2, 3)
- Pessimistic
- Zeropool.network

We also appreciate the help of Scott Bigelow and 1inch team for doing a security review of the smart contracts.